Comparative Review: CDP p.21

Mark Minasi's Power Tools p. 67

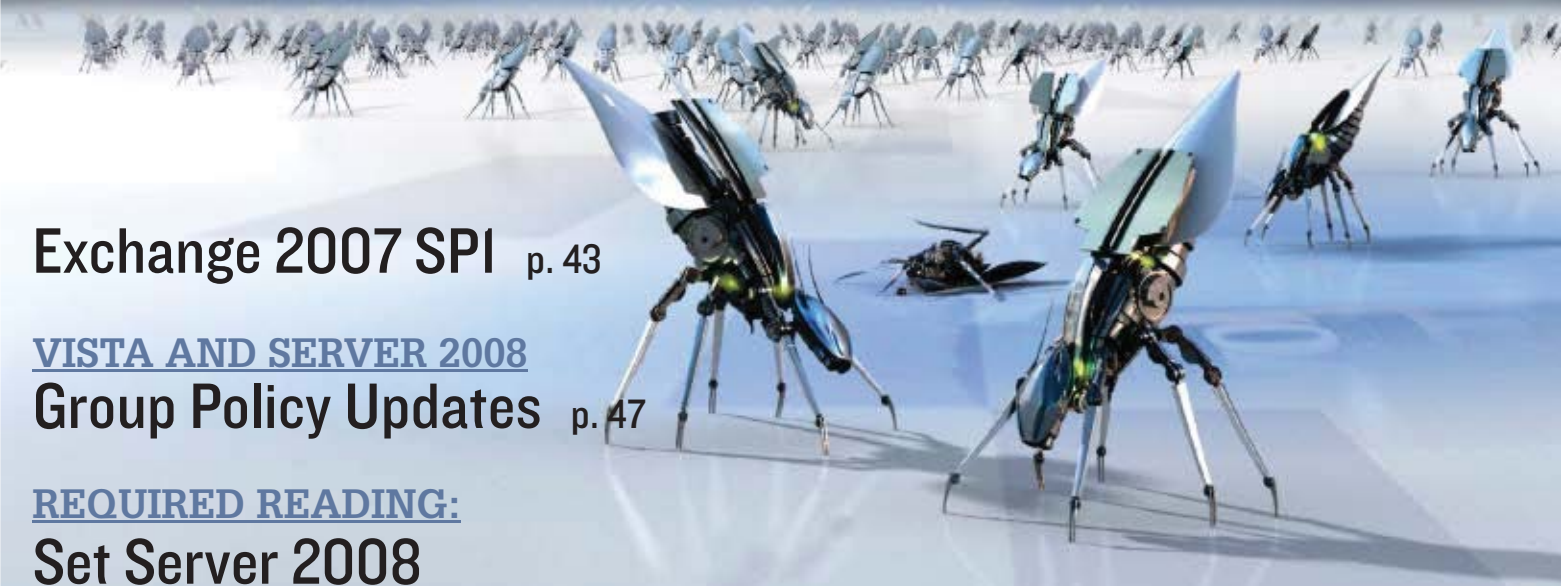
MANAGEMENT • SECURITY • NETWORKING • MESSAGING • HOW-TO

Windows® IT Pro

We're in IT with You

January 28, 2008
EXCHANGE 2007
Mastery Series
SEE PAGE 52

SQUASH PESKY IT ANNOYANCES



Penton
A PENTON PUBLICATION

JANUARY 2008
WWW.WINDOWSITPRO.COM
U.S. $5.95 CANADA $7.95

Windows IT Pro
JANUARY 2008 VOLUME 14 NO. 1

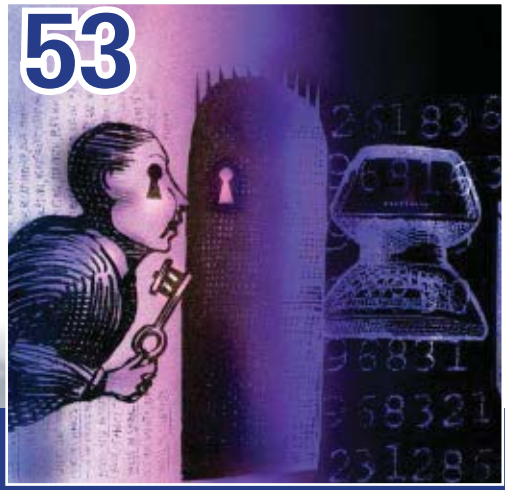
FOCUS

COVER ILLUSTRATION BY RYAN ETTER

FEATURES

OFFICE & SHAREPOINT PRO

TRICKS & TRAPS



Access articles online at www.windowsitpro.com. Enter the article ID (located at the end of each article) in the InstantDoc ID text box on the home page.

"I had been using Microsoft Visual Source Safe (VSS) for some time, but VSS began driving me crazy . . . I began looking for a better solution."
—Les Pinter, Founder, Pinter Consulting

PRODUCTS

WHAT'S HOT

IN EVERY ISSUE

COLUMNS

Karen Forster
IT Pro Perspective
Microsoft System Center Configuration Manager
Microsoft knows that the number one cause of unplanned downtime on Windows Server is configuration changes that cause unforeseen problems. SCCM is meant to address such problems and free IT to do things like deploy Windows Server 2008.

Mark Minasi
Windows Power Tools
Protect Your Data with Cipher
To get a real sense of EFS's file-protection power, you need to be using the command-line encryption/decryption tool Cipher. Here's an overview of Cipher's syntax and options.

Paul Thurrott
Need to Know
How Windows Server 2008 Developed, Part 2
This exclusive behind-the-scenes look at how Microsoft works draws on inside information from the go-to guy in charge of the Server 2008 schedule, Alex Hinrichs.

Michael Otey
Top 10
Windows Vista Annoyances
User Account Control isn't the only thing frustrating users of Windows Vista. You've also got to worry about software and hardware incompatibilities and a system that doesn't always remember your preferences.

It's a small world after all...

Your organization is global and so is your IT infrastructure. Some days that means you need to operate and solve problems in 12 time zones. With Avocent, you can solve most any crisis that the network gremlins can throw at you without leaving your desk or using your passport.

Avocent infrastructure solutions put complete manageability at your fingertips. We've combined our innovative and powerful hardware and easy-to-use software to enable remote access and control of literally any system on the planet. At anytime. From anywhere.

Download our white paper today and find out how you can manage your physical and virtual world from one common interface. Visit **www.avocent.com/itpro**

Avocent®

WindowsDeveloperPro: Share Your Experiences

Send us your real-life stories about how developers and systems administrators creatively solve classic problems such as lowering maintenance costs and simplifying application development. Email your contributions (with "Reader to Reader" in the subject line) to sheila.molnar@penton.com. Please include your full name and phone number. If we publish your submission on WindowsDevPro.com, you'll get $50!

Check out our onsite and virtual events covering Microsoft Exchange Server, SharePoint, virtualization, business intelligence (BI), and more!

www.windowsitpro.com/events

Ensuring User Continuity

Companies that implement true high availability and disaster recovery solutions protect the continuity of their business. Learn how to keep your users and your business up and running, differentiate alternative HA/DR solutions in the marketplace and determine what works for you, and ensure user continuity through seamless recovery of your key systems and data.

www.windowsitpro.com/go/seminars/neverfail/usercontinuity/?code=citcjan

YOUR SAVVY ASSISTANT

The Missing Link to IT Resources

www.windowsitpro.com/go/SavvyAssistant

BY CHRISTAN HUMPHRIES

Put Out by IT Outsourcing

It's cold here. And there's a strange smell coming from a dish beside the monitor. But I can't think now about my discomfort or what in the world is in that bowl. I must finish my work, and I have only minutes before she discovers me using her computer. With a broken PC and no help from the *Help* desk, I've been reduced to a PC parasite: a lonely vagrant feeding on others' machines after they've gone home—or even to lunch.

A year ago I didn't have to lurk in the shadows of our beige hallway, waiting to pounce on an unoccupied PC. If my machine broke down, I could just call our onsite technicians. But our company is now outsourcing IT, and the only person who can help me is away on business.

A thread in our Career Development and Job Opportunities forum asks whether outsourcing is good or bad, and forum member meyercl3 answers, "In my experience, bad for the organization . . . The outsourcer wants to do as little as possible to meet the terms of the contract in order to maximize their profitability." From what I've seen so far, I have to agree.

I'm not saying that my PC is busted because we're outsourcing. I'm not even saying that the IT contractors won't fix it soon. I'm just saying that this "efficient" money-saving business move sure hasn't helped.

Has outsourcing put you out—of a job, of your mind? Comment on my extended blog post at InstantDoc ID 97705, or email me at chumphries@windowsitpro.com.

Help (Desk) Yourself

Are you dealing with helpless end users like me? These resources can help keep them out of your hair.

"Cut Down on Calls to the Help Desk," August 2005, InstantDoc ID 46951

"42 Tips to Empower Your Office Users," May 2006, InstantDoc ID 49742

JSI FAQ site, www.jsifaq.com

Special Operations Software™

Power your Active Directory to new heights

Specops Command

PowerShell remoting through Group Policy

"Psychotically Powerful"

Specops Command ™
We bring you the future of scripting, today!

Specops Deploy ™
Group Policy based
Software Deployment

Specops Inventory ™
Group Policy based
Asset Management

Specops Password Policy ™
For Multiple Password
Policies in AD

Active Directory Janitor ™
Keeps your Active
Directory clean

Microsoft GOLD CERTIFIED Partner

Security Solutions
ISV/Software Solutions

For more information about Specops Command and to download your FREE limited version or full trial version please go to:
www.specopssoft.com/powershell

Microsoft System Center Configuration Manager

Making IT a business asset

It's common knowledge that IT people spend about 70 percent of their time on maintenance tasks. But just think of all the projects you could finish and how much you could benefit your organization's bottom line if you could reduce that percentage. Freeing IT from day-to-day drudgery so that technology can become a strategic business asset is a key motivator behind Microsoft's efforts to unify its systems management products and management infrastructure. The System Center family is at the core of these efforts. The recent release of System Center Configuration Manager 2007 (SCCM) illustrates Microsoft's focus on "transforming [customers'] infrastructure into a strategic and progressive asset for their business," according to Brad Anderson, general manager of Microsoft's Management Solutions Division.

For example, Brad said, "We know that the number-one cause of unplanned downtime on Windows Server is when a configuration change is made and the ramifications [of that change] are not truly understood." With the model-based management approach built into SCCM, Brad continued, "we'll have technology in place so when a configuration change is made, we'll be able to detect that the change was made and notify the administrator before that change becomes a catastrophe." The idea is that by identifying the causes of common problems and providing ways to avoid them, System Center can have "dramatic impacts on uptime, customer satisfaction, and real value to the customer."

To illustrate the value of System Center's capabilities, Brad cited the example of a study examining Microsoft's customer-support calls. "In January 2007, we looked at every call that came in about our big server workloads in the most critical situations—when the customer is literally down and in need of help. We looked at how many of those calls would have been avoided, and 48 percent of all those critical calls would have been prevented had [the customer] been using the monitoring capabilities of Operations Manager and the desired-configuration management capabilities of Configuration Manager."

Those capabilities, Brad continued, are based on "models that instruct System Center how to verify compliance and any deviation, or drift, from a desired state. Microsoft and some of our partners will be releasing models, and there will be tools for IT professionals to customize those models and build their own. They can build a model for almost anything: How should a server be configured? What does a secure desktop look like? The way we envision this is the developer—whether that's internal or an ISV—will release their products with a model for how the application should be configured. But then IT professionals may choose to extend that, enhance it, change it, based on their criteria. We also see IT professionals take an application model and combine that with an OS model and a compliance model. And that is what they'll use to see if a server, for example, is configured properly."

Windows Server 2008

Of course, one important reason why Microsoft wants to free up your time from maintenance is to give you time for tasks such as deploying new versions of Microsoft products—Windows Server 2008, for example. And Brad's team "has the responsibility to make sure that enterprise accounts have a simple and efficient way to deploy Windows Server and upgrade to Server 2008 across the enterprise." So it's no coincidence that SCCM is being released almost simultaneously with Server 2008.

Brad reported that "In our TAP [Technology Adoption Program] deployments of SCCM, the feedback we got for the OS deployment capabilities is that it truly does enable everything from configuring the hardware, to making sure the server is ready to be upgraded, to doing the deployment or upgrade—and then after you're done, bringing back the applications, bringing back the configuration, joining the domain, configuring the server so it's ready to go. So one of the ways people will be using SCCM is that base configuration."

Freeing IT from day-to-day drudgery is a key motivator behind Microsoft's efforts to unify its systems management products.

Brad admitted, "Asking our customers to upgrade from one version of Windows to another is one of the most complex things we ask them to do." He added, "We're pretty proud of what we've delivered in SCCM 2007 to help our enterprise accounts get upgraded to Server 2008."

In summary, Brad said, "We have delivered technology to the market that enables that connection between IT and the developer and allows the IT organization to really understand what's happening on their desktops, their servers, and the applications they run on those."

InstantDoc ID 97656

Karen Forster (karen@windowsitpro.com) is editorial and strategy director for *Windows IT Pro* and *SQL Server Magazine* and former director of Windows Server User Assistance at Microsoft.

_INFRASTRUCTURE LOG

_DAY 84: Feeling really disconnected. We're not getting the most out of our existing assets. Service and application integration is a nightmare. We've got to stop working on these islands.

_Please rescue me from this lack of connectivity.

_DAY 87: We're saved! With IBM WebSphere solutions we can service-enable and connect our existing assets for mission-critical goals. Now we can reuse existing applications and save money by eliminating redundant systems. We're ready for any SOA integration project.

_Plus, no more jellyfish stings.

WebSphere®

Download the enterprise service bus white paper at:
IBM.COM/**TAKEBACKCONTROL**/CONNECT

EDITOR'S NOTE

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

Group Policy for Everyone

Eric Rux's "3 Tools to Manage Group Policy" (November 2007, InstantDoc ID 97228) is a great article. I didn't find a wasted line of text. Eric explains things so that a systems administrator at my level—that is, the kind who knows enough to be dangerous—can easily follow along. Users at higher skill levels—say, Mark Minasi's level—will also find something valuable. There's great information here for everyone, regardless of skill level. Keep these articles coming!

—Tim Bolton

IT Innovator Illusion

Maybe I'm late to the party, but it seems to me that that the *Windows IT Pro* November 2007 cover illustration should qualify for your Ctl+Alt+Del section. If those three gears in the IT innovator's head actually move, all he'll get is metal shavings and broken teeth. Two interlocked gears can't move in the same clockwise/counter-clockwise direction, so three interlocked gears can't move at all.

—Benjamin R. Wahlquist

16 Flavors of Windows Server 2008

I read Paul Thurrott's Web-exclusive article "Microsoft Muddies the Windows Server 2008 Waters" (November 13, 2007, InstantDoc ID 97570). As a longtime Windows server administrator, I look forward to the Server 2008 product. But why is Microsoft making things so confusing and murky lately? Honestly, doesn't someone at Microsoft have common sense? No one benefits from 16 flavors of Server 2008. Microsoft is making better products, but some of the company's recent decision-making and marketing choices are enough to make you scratch your head.

—COMPWIZ

Ready to Deploy Vista?

In her online column, "Windows Vista Deployment News: ROI Study, MDOP, BDD, Springboard" (November 15, 2007, InstantDoc ID 97599), Karen Forster asks, "What does Microsoft need to do to convince you to deploy Windows Vista?" I'm not convinced that Microsoft has the tools a domain administrator needs to manage a domain from within Windows Vista.

I think Microsoft needs to put up a virtual "Domain Administration with Vista" lab that features all the technology the company can provide. I know the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in isn't up to par, as outlined in the Microsoft article "You experience installation errors and compatibility problems when you install Windows Server 2003 management tools on a Windows Vista-based computer" (support.microsoft.com/?scid=kb;en-us;930056&x=13&y=13). I talk about this problem in my Scripting Pro VIP article "Using Saved Queries for Active Directory Management" (October 2007, InstantDoc ID 97087). If Microsoft were to indeed embark on this kind of lab, the company would need to make its follow-up feedback pages oriented more toward customer satisfaction than marketing.

I'm also a bit concerned about Vista compatibility with older hardware such as old HP printers, legacy scanners, and expensive plotters. People and companies won't want to spend a lot of money on new equipment just so they can have a newer OS.

—Jim Turner

Women in IT

In "Can You Hear Me Roar Now?" (Your Savvy Assistant, October 2007, InstantDoc ID 97461), Christan Humphries asks whether women are shut off in the IT community. They aren't shut off from *my* IT community. I recently hired an assistant—one bona fide, technical assistant, qualified and ready to work. When I was looking for a new employee, one of my personal goals was to hire, yes, a woman.

In a two-"man" shop, I understand the different kind of thinking that a woman can bring to IT processes. I acknowledge that women solve problems differently than men do. I can also see that women tend to be more compassionate to end-users. Whereas I might lose patience with a user who has forgotten "his" password for the 27th time, she thinks it's funny and moves on. Don't even get me started on how women approach training. I could go on and on about the benefits that women bring to the table in the IT world.

However, when considering the lack of female winners for IT Innovators (*Windows IT Pro*, November 2007), you need to look at the sheer numbers of men versus women in IT before you start lamenting that all the winners were men. We can't simply ignore an innovator because we don't have enough females on the list. How would you feel if you were put on the list of innovators not because you were an innovator but because somebody thought they needed a "token" female on the list to appear politically correct? If you start putting one gender before another, you're simply going back to what we had before: gender bias.

—Scott Gutauckis (MALE)

InstantDoc ID 97711

Learn how to make your data center more efficient:
IBM.COM/**TAKEBACKCONTROL**/GREEN

1. Requires Advanced Power Virtualization, which is optional and available at an additional charge. IBM, the IBM logo, Cool Blue, POWER6 and Take Back Control are trademarks or registered trademarks of International Business Machines Corporation in the United States and/or other countries.

What You Need to Know About ...

How Windows Server 2008 Developed, Part 2

Paul Thurrott
(thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

Last month, I presented part one of an exclusive, behind-the-scenes look at the creation of Windows Server 2008 with Alex Hinrichs, the Windows Server 2008 project manager (see "What You Need to Know About How Windows Server 2008 Developed," December 2007, InstantDoc ID 97400). Hinrichs runs the Windows Server ship room and manages the development of this increasingly complex product line. This month, I continue my interview with Hinrichs. Here, then, is more of what you need to know about the development of Server 2008.

Stepping Into the Ship Room

"It's real simple," Hinrichs told me. "You walk in each morning and find out what is the state of the main build. We build it overnight. Did the build break any of the BVTs [build verification tests] or the thousand or so self-host tests we run? We look at the state or health of the daily build."

Build breaks are very rare, Hinrichs said. In such a case, errant code from further down the tree can break dependencies or functionality in the main build, causing a temporary build cessation while the suspect code is found. Although this calamity occurred many times during the development of Windows Server 2003, it's only happened once or twice to Server 2008.

"The day-to-day focus of [the ship room] until fall [2006] was Windows Vista," Hinrichs said. "Here on Server, we kind of rode along for the ride. But once Vista was done, there was a changing of the guard almost immediately, and I took over ship room." Now, he said, Server 2008 and Vista SP1, which are being developed in tandem, are the focus. "Starting from Vista RTM [release to manufacturing, in early November 2006], we flipped the switch pretty quick," he added. "It was like two aircraft carriers passing each other. But working from the Vista RTM code gave us a very stable code base, so we were able to go full bore from the get-go. We have been able to create a stable main build every day since then, since most of the problems are trapped before they even get here."

Locking Down the Code

In keeping with their habits of learning from the past, the Windows Server team carried over another bit of wisdom from their experiences on Windows 2003: They locked down the code for this product fairly early in development. "We locked down the feature list at end of 2006," Hinrichs said, noting that a change-management process was then set up so that anyone who wanted to make a change request would have a formal process to follow. "We have a board consisting of me, Iain [McDonald], and Bill Lang [Iain's boss]," Hinrichs told me. "When someone wants to make a functional change to the product, they meet with us. We weigh the consequences of those changes."

Most changes aren't accepted, as the Server team is leery of feature creep, which it feels created problems on early Windows Server versions. Now, developers can't just check in new code on a whim: Microsoft has quality gates in place, up and down the code tree, to monitor what's coming in. "We worked hard to maintain the feature list we finalized and have only taken in changes that were either blocking deployments or because the business case was so compelling we simply had to," Hinrichs confided.

This raises an obvious question: Which features were added after the late 2006 functional freeze and which were not added? Hinrichs wasn't particularly keen on discussing what wasn't added to Server 2008, for obvious reasons, but one change the team made does stand out: Very late in the development of Server 2008, the team decided that it simply had to add Windows PowerShell to the product, even though the existence of two scripting and command-line environments, one of which (PowerShell) wouldn't be fully supported with built-in management tools for all of the product's capabilities, would be confusing to some customers.

"This is precisely the type of thing we reject," Hinrichs admitted. "You don't want to randomly add some new administrative tool to the product so late in the game, and there's no way to create the necessary PowerShell scripts after Beta 3 [which was when PowerShell was added to Windows Server]. We already had command-line tools and had significantly improved the traditional command-line environment in Windows Server 2008. So it was a tradeoff. We're committed to PowerShell, and love it, and we wanted it in the box. But we didn't want to slip the release date just to add some administrative scripts for PowerShell. We're not going to add gravy."

On the flipside, after Microsoft revealed the Server Core installation option for Server 2008, its customers immediately began providing the company with feedback about other roles they wanted to see added. The number one requested role was Web Server. But because Server Core doesn't support the Microsoft .NET Framework in this release, there was no way to create a version of the Microsoft IIS Web server for that environment that supported dynamic capabilities such as ASP.NET. The Windows Server team decided instead that it would support a Web Server role in Server Core and that Server Core version of IIS won't support any .NET-oriented features in the first release. The

IT'S A PERFECT FIT!

INTRODUCING THE STOREVAULT S300 FOR UNDER $3K

ENTERPRISE TECHNOLOGY FOR YOUR SMALL BUSINESS STORAGE NEEDS

If you are looking for instant back up and data recovery, with RAID DP protection against dual drive failure, you've found the perfect fit. With NAS, iSCSI SAN, and DAS right out of the box, the StoreVault product family provides storage solutions that will grow with your business needs. NetApp enterprise-proven technologies provides a rich feature set, including simple on-the-fly provisioning and off-site data replication. It's truly the perfect fit to maintain business continuity and regulatory compliance.

The new **S300** starting at under **$3,000**
or the **S500** starting at **$5,535**

Call us today at 800-206-5363
Learn more about our **Special Offers**
at **www.storevault.com**

NetApp®

StoreVault™
A NetApp Division

result is a low-impact version of IIS that's super secure. Customers were ecstatic, as what they were looking for in this space was a low-end Web server solution that could compete more effectively with Linux-based solutions.

"The feedback from Beta was pretty clear," Hinrichs said. "Customers told us, 'Wow, this Server Core thing is fantastic, I love it, but you missed the most important role.' So we went and took care of that."

> "That was the genesis of componentization: Cut the dependencies and arrive at a smaller, more pared-down version of the OS. It runs lean and mean."
>
> —Alex Hinrichs, Windows Server 2008 project manager

Adding IIS to Server Core was a big undertaking but worth the effort because IIS impacted so many customer deployments. PowerShell, by comparison, is something the company is moving toward supporting more pervasively across Windows Server but felt it wasn't absolutely critical to have a complete set of admin scripts in the initial release (they can ship after the fact via the Web). It would be nice, but it's not critical. It's worth noting that Microsoft will indeed support PowerShell with a full suite of administrative scripts via a Web-based library concurrently with the release of Server 2008. (Hinrichs noted that an amazing community of PowerShell users has already sprung up; this group, too, will no doubt supply users with useful and compelling scripts for that environment.)

Working with Customers

One of the most amazing changes in the manner that Server 2008 was developed is the way that the team has integrated customer feedback so thoroughly into the process. "The old way of doing this was that customers would file beta bugs, and then we'd have call downs and onsite customer visits," Hinrichs told me. "We still do those things, of course. But on top of that, we can now process CEIP [customer experience improvement program] data, which is information that comes back from the servers that are installed around the world. This information, which is strictly opt-in, is pumped back to Microsoft so we can study it."

It's a considerable amount of data. Microsoft received CEIP data from over 165,000 installations of Windows Server 2008 Beta 3, which shipped in late April 2007. The company knows how many customers have installed Beta 3 and even exactly what roles they installed. And yes, I can tell you what those are: Percentage-wise, the most popular Server 2008 roles are Active Directory (AD), Web Server, File Server, and Terminal Services.

Server 2008 also supports the notion of features, which are functional components that aren't as broadly defined as roles. The most popular features so far are PowerShell and, surprisingly, Desktop Experience, the latter of which allows the Server 2008 desktop to look more like Vista. Hinrichs told me that people had complained about the feature in Windows 2003, so the team carved it off of the default installation so that those who wanted it could install it separately. These people are typically enthusiasts, he said.

The Windows Server team also sees which combinations of roles are getting installed on the same server and which architecture (x86 or x64) people are installing. "We know that x64 is what all customers are buying now and in the future," Hinrichs said. "The deployments are all x64. There is some testing on 32-bit [x86], but we also know that many of these are in virtual machines [which tend to be 32-bit only]. So we put our testing and development wood on x64. The CEIP really helps us know that we have the right focus and priorities."

Customer feedback also helped Microsoft determine the feature set for Server 2008. "That was actually the origin of Server Core," Hinrichs told me. "Customers were saying that there are all these services running they don't need, all these extra components. They were installing QFEs [hot fixes] that had nothing to do with server roles they're running. That was the genesis of componentization: Cut the dependencies and arrive at a smaller, more pared-down version of the OS. It runs lean and mean and doesn't need a GUI, Internet Explorer, or the .NET Framework." That said, Microsoft is also evaluating changing the supported component mix in Server Core for the future based on customer feedback.

Read-Only Domain Controller (RODC) is another example of a Server 2008 feature that arose out of customer feedback, this time from enterprise customers. "They said they loved Active Directory but had branch offices all over the world," Hinrichs said. "Replicating across the WAN was painful. Maybe they had a head office in New York and an oilrig in Kazakhstan. They don't want all of their passwords replicated to that remote location. Read-Only Domain Controller caches passwords only for the people who log on in that location. They're not giving up the goods if they get compromised."

Calm Before the Storm

As a long-time Microsoft observer, I noted to Hinrichs that the Server 2008 development process, although lengthy, seemed to lack the drama and disappointments that marred Vista. He wasn't particularly interested in making direct comparisons with the Windows client team, but he did tell me that the calmness exuded by the server team is a direct result of the quality and maturity of the team they have in place.

"It may seem calm on the outside," he said, "but that's because we have a lot of senior people on Windows Server, including some folks who shipped many versions of Server over time. They are very effective at planning and managing their businesses, and they deliver what they promise. The seniority factor really helps."

"The other thing is that Server people are Server people," he added. "We just love working on Server. We haven't had a hard time retaining people at all."

Hinrichs also credits the team's clear focus on server roles as a factor in the clarity of the

product's development. "This isn't BS," he said. "We get a lot of steadiness from Bob [Muglia], Bill [Lang], and Iain [McDonald]. They're steady, and their world is steady. We go to ship room, we set milestones, and we figure out how to work with the teams. We tried hard to be consistent, and maintain a consistent rhythm."

Part of this rhythm involves some of the little things that other organizations simply don't get. For example, employees aren't asked to work most weekends. "We tried things that way, once," he said. "It didn't work."

The result is indeed a smoother running organization. When Microsoft shipped Server 2008 to almost 1 million people, with 1,000 external real-world deployments and 600 internal deployments, the Windows Server team sat back and wondered whether the complaints would come pouring in. It never happened. "The builds are just so solid," Hinrichs told me. "There's just nothing major wrong. We haven't had a million customer problems."

Hinrichs told me that the executive in charge of the Technology Adoption Program (TAP) is on call with all of the Fortune 500 companies that are deploying pre-release Server 2008 versions in production. They have his cell phone number and can call him 24 x 7," he said. "Remotely or via a plane trip to visit them on-site, he will fix whatever problems they're having. He's only been woken up once in the last six months. That's it. That was not the case with previous Server releases."

One area where Server 2008 has, perhaps, veered a bit off course, however, is with Windows Server Virtualization technologies, code-named Viridian. This feature is now due in public beta form when Server 2008 ships in first quarter 2008 and will appear in final form within 180 days of that date. Hinrichs, curiously, wasn't interested in taking the easy out on this one, even though Viridian was actually being developed outside of the Windows Server team for much of its existence and was only recently pulled into the core OS team.

"It was a parallel project, but we're just glad we have a CTP [Community Technology Preview, which appeared in Release Candidate 0] so that folks can have an early look," he said. "Some parts of Windows Server 2008 have been stable for a very long time, like IIS, which began a Go Live program before Beta 3. Active Directory is the same thing."

Final Thoughts

Although many have noted that the gestation time for Server 2008 was lengthy even by Microsoft standards, the resulting product appears to address customer needs and achieve a level of stability and reliability that has thus far largely escaped the Windows client product. It seems that the extra time has been well spent—though Server 2008 will arrive in the market five years after the previous major Windows Server release, it's coming with an array of customer-driven functionality such as Server Core, RODC, a more modular IIS 7.0, and integrated virtualization support. Microsoft often talks up its interactions with customers, but in this case, this partnership appears to have worked wonders with the development of Server 2008.

InstantDoc ID 97549

EDITOR'S NOTE

Share your Windows discoveries, comments, solutions to problems, and experiences with products and reach out to other *Windows IT Pro* readers (including Microsoft). Email your contributions to r2r@windowsitpro.com. Please include your phone number. We edit submissions for style, grammar, and length. If we print your submission, you'll get $100. Submissions and listings are available online at www.windowsitpro.com. Enter the InstantDoc ID number in the InstantDoc ID text box.

How to Get Information About Installed Applications Without Using WMI

Some Windows Vista systems have Windows Management Instrumentation (WMI) queries of the Win32_Product class fail and provide the less-than-helpful message *Generic failure*. Repairing WMI typically doesn't solve the problem. In a Usenet group discussion, Microsoft insider Jeffrey Snover confirms that this is a known bug scheduled for a fix in Vista's SP1 (see groups.google.com/group/microsoft.public.windows.powershell/browse_thread/thread/a3313bfdeaaca2af/66061dcb9ea6578a).

In one post in the discussion, Keith Hill mentions that you can get the same information that the Win32_Product class provides directly from the registry. The Win32_Product items are all in subkeys under the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall key. However, Hill doesn't mention how to extract the data. Depending on what tools you're comfortable with using and what you need to do, there are a few options for quickly extracting the data. These options aren't limited to Vista. You can use them on other Windows OSs if you're having problems with the WMI subsystem.

If you want to save the data in a file for later use, a simple approach is to run regedit, navigate to the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall key, right-click that key, and select Export from the context menu. You can then save the data in a .reg file.

If you want to display the data, you can use command-line tools. One such tool is reg.exe. After opening a command-shell window, run the command

```
reg query HKLM\SOFTWARE\
  Microsoft\Windows\CurrentVersion\
  Uninstall /s
```

(Although this command appears on several lines here, you would enter it on one line. The same holds true for the other multiline commands presented here.)

Another command-line tool you can use is Windows PowerShell. In PowerShell, the simplest way to display the data is to use the Get-ChildItem cmdlet (which has the alias of gci), then pipe its results to the Get-ItemProperty cmdlet. (Get-ChildItem doesn't retrieve information about the registry values contained within subkeys; it only lists the subkeys' names.) So, the command that you'd enter in the PowerShell window would be

```
gci "HKLM:\SOFTWARE\Microsoft\
  Windows\CurrentVersion\Uninstall" |
  ForEach-Object{Get-ItemProperty
  $_.PSPath}
```

You can filter the output of this command to make it more readable by piping the output to the Select-Object cmdlet, putting the names of the properties you're interested in as arguments. For example, here's how I use Select-Object to get some of the more useful information from the registry keys:

```
Get-ChildItem HKLM:\SOFTWARE\
  Microsoft\Windows\CurrentVersion\
  Uninstall | ForEach-Object{
  Get-ItemProperty $_.PSPath} |
  Select-Object DisplayVersion,
  InstallDate,ModifyPath,Publisher,
  UninstallString,Language,
  DisplayName
```

On the *Windows IT Pro* Web site, you can download a couple of scripts—GetApplicationUninstall.cmd and Get-ApplicationUninstall.ps1—that automate getting the product information from the Uninstall key. (Go to www.windowsitpro.com/Windows/Article/ArticleID/97604/97604.html and click the *Download the Code Here* button near the top of the page.) You can run GetApplicationUninstall.cmd, which uses reg.exe, from a command prompt to display the output from the local machine. If you add the name of a remote machine to the command line, the data will be returned for that remote system. Get-ApplicationUninstall.ps1 is a native PowerShell script that runs only against the local system.

Admittedly, all three workarounds aren't ideal because they're just data dumps. However, they at least provide a way to get information about a machine's installed applications when you can't use WMI.

—Alex K. Angelopoulos
Senior Network Engineer
InstantDoc ID 97604

PowerShell Script Lets You Check Patches' Status

Each time Microsoft Software Update Services (SUS) downloads patches, there are always a few machines not properly patched due to unforeseeable problems. Because SUS doesn't have any reporting tools, it's difficult to determine which machines aren't patched. Thus, administrators at my company have been using KB.vbs to report the status of patches on more than 600 Windows client machines. In my Reader to Reader article "Does SUS Make You Want to Send an SOS?" (www.windowsitpro.com/Articles/ArticleID/46953/46953.html), I present this VBScript script, which I wrote.

Although KB.vbs works well, I decided to rewrite the script in PowerShell last July because I wanted to experience the *power* in PowerShell firsthand. More important, I never want to stop learning. I feel it's important to learn to apply PowerShell to current problems.

The result is kb.ps1. Like KB.vbs, kb.ps1 first attempts to ping the machines listed in an input file named pclist.txt. If a PC is online, the script determines whether the specified patch exists and reports the results. To make it easier to spot problematic computers, the names of the computers that aren't patched are displayed in red and the names of the computers that are successfully patched are displayed in green. The script also reports ping failures.

NEW RELEASE

"This is by far the best defrag product… After installing Diskeeper 2008 I don't have to worry about disk fragmentation ever again. It does everything for me invisibly in the background."

Jozo Capkun, *President*
Komoko Services Limited

It's Smart.
It's Transparent.
It Will Take Your System From Zero to Sixty—*Automatically!*

Automatically and invisibly solve disk performance issues—forever

File fragmentation—the splitting of files in tens, hundreds or thousands of pieces—puts the brakes on system performance. It slows access to a crawl. It causes delayed application launches and slow boot ups. It can even cause system crashes.

Introducing the first and only completely automatic defragmentation solution. New Diskeeper® 2008 with InvisiTasking™ defragments in real-time, invisibly in the background. Intelligently monitors and utilizes only idle system resources, while users continue to work. And with fragmentation completely eliminated, your performance flies. Systems are maintained at peak performance and reliability—*automatically!*

- ***True transparent, background defragmentation,*** *unnoticeable to applications and users—except, of course, for the newfound performance and reliability.*
- ***No scheduling required.*** *Ever. Ever. Ever.*
- ***Adaptive technology boosts access*** *to your most commonly-requested files, beyond defragmentation alone.*
- ***Work smarter not harder.*** *Each volume is different. Dynamic intelligence determines and delivers maximum minute-to-minute benefits with minimal effort.*
- ***Advanced defragmentation*** *uniquely designed for high-capacity, high traffic disks.*
- ***No room to move? Extreme fragmentation? No problem.*** *New, complete defragmentation in all conditions—even with less than 1% free space.*
- ***Critical system file fragmentation*** *now automatically prevented.*
- ***Allows you to leverage VSS data protection*** *and the performance and reliability of defragmentation.*

FREE OFFER

NEW *with InvisiTasking™*
Diskeeper® 2008
Maximizing Performance and Reliability—*Automatically™*

Try New Diskeeper 2008 Free for 45 Days!

Download at www.diskeeper.com/win2008

Note: Special 45-day trialware is only available at the above link

Volume licensing, government and educational discounts are available from your favorite reseller. For a free quote visit www.diskeeper.com/quote10 or call 800-829-6468. *Code 4006*

Diskeeper corporation

Figure 1 shows a sample input file. The path to this input file and the patch to search for are specified on the command line when you launch the script. The launch syntax is

```
powershell.exe Path\kb.ps1
  InputFilePath kbxxxxxx
```

where *Path* is the folder in which kb.ps1 is stored, *InputFilePath* is the pathname of the input file, and *kbxxxxxx* is the ID of patch you want to search for. Alternatively, if kb.ps1 and pclist.txt are in the same folder in the default PowerShell directory (e.g., D:\PowerShell\scripts), you can type

```
Path>powershell .\kb.ps1
  .\pclist.txt kbxxxxxx
```

where *Path* is the folder in which kb.ps1 and pclist.txt are stored and *kbxxxxxx* is the ID of patch you want to search for.

As Listing 1 shows, kb.ps1 starts by executing two commands that you wouldn't typically see at the beginning of PowerShell scripts. The first command

```
$erroractionpreference = `
  "SilentlyContinue"
```

```
pc-00001
pc-00002
pc-00003
pc-00004
```

Figure 1: Sample input file

completely suppresses error output. By default, when an error occurs, PowerShell issues an error message, then continues to the next line. When you set the $ErrorActionPreference automatic variable to SilentlyContinue, the processing continues but an error message isn't issued. Suppressing error messages eliminates distractions for the administrators when they're reviewing the onscreen patch-status report. Because kb.ps1 is a tried-and-true script that we've been using continually for the past 6 months, the benefits of suppressing error messages outweigh the risks.

The second command

```
clear-host
```

clears the PowerShell window. Typically, the Clear-Host function is used at the end of scripts, but I used it at the beginning of kb.ps1 to clear the screen before any processing begins. Once again, that helps generate a clean, easily readable electronic report for administrators to review.

After clearing the PowerShell window, kb.ps1 counts the number of command-line arguments. If there aren't exactly two, it displays the syntax for the launch command. If two arguments are present, the script retrieves them, assigning the input file pathname to the $filename variable and the patch ID to the $kb variable.

Using the Get-Content cmdlet, kb.ps1 reads in the names of the computers in $filename, one at a time. For each computer, the script uses Windows Management Instrumentation's (WMI's) Win32_PingStatus class to ping the computer. The Get-WmiObject cmdlet with the -query parameter is used to execute the WMI Query Language (WQL) statement that pings the machine. The script determines whether the ping succeeded (i.e., returned a value of 1) by checking the value in the StatusCode property of the Win32_PingStatus class.

If the ping didn't succeed, kb.ps1 uses the Write-Host cmdlet to log the computer's name and the message *Ping failed*. I didn't use the Write-Error cmdlet to write the ping-failure information because it mangles the information almost to the point of being unreadable. After writing the error message, the script ends so that the Help desk can determine why the machine is offline and fix the problem.

If the ping succeeded, the script uses the Get-WmiObject cmdlet with WMI's Win32_QuickFixEngineering class to retrieve the patches installed on that computer. The script pipes the results to the Where-Object cmdlet, which filters the results for information about the specified patch. The results of that filter operation are then piped to the Select-Object cmdlet, which retrieves the patch's HotFixID and Description properties.

As callout A shows, kb.ps1 checks to see whether the HotFixID property's value is the same as the $kb variable's value. If they match, the script writes the computer's name and the patch's description in green text. If they don't match, the script writes the computer's name and the message *Patch not found* in red text.

To write the patch-status information, the script again uses Write-Host. This cmdlet writes information directly to the host interface, which makes the output unusable for pipelining. However, we don't need the output piped anywhere. Equally important, if the script were to let standard output handle the patch display, you'd get lots of pages containing extraneous information. For our purposes (i.e., generating a clean, easily readable electronic report), using Write-Host works best.

As you can see, there's nothing fancy about kb.ps1. However, it's shorter and faster than KB.vbs. Plus, the color-coded results make the report easier to read and more presentable for administrators.

—James Lim Kah Kheng
Lead System Engineer, NOL

InstantDoc ID 97609

Listing 1: Kb.psl

```
$erroractionpreference = "SilentlyContinue"
clear-host

if ($args.count -lt 2)
  {
    write-host -f blue "Syntax Error : Must have 2 parameters."
    write-host -f blue "Eg powershell.exe <path>\kb.ps1 <pathname of file> <kbxxxxxx>"
    break
  }

$filename = $args[0]
$kb = $args[1]
$computernames = get-content $filename

foreach ($computer in $computernames)
{
  $strQuery = "select * from win32_pingstatus where address = '" + $computer + "'"
  $wmi = get-wmiobject -query $strQuery
  if ($wmi.statuscode -eq 0)
  {
    $checkkb = get-wmiobject Win32_QuickFixEngineering -computer $computer | `
      where-object {$_.hotfixid -eq $kb} | select-object hotfixid, description
A   if ($checkkb.hotfixid -eq $kb)
      {write-host -f green $computer "`t" $checkkb.description "`r"}
    else
      {write-host -f red $computer "`t" "Patch not found." "`r" }
  }
  else
    {write-host $computer "`t" "Ping failed." "`r"}
}
```

EDITOR'S NOTE: Send new product announcements to products@windowsitpro.com.

Product Spotlight

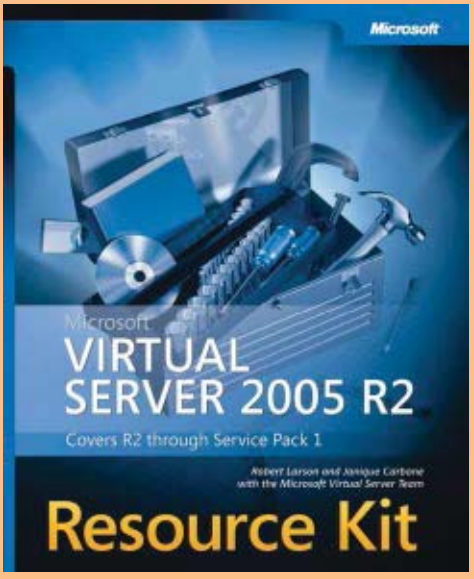
Exchange/Messaging

Support GAL Lookup on Mobile Phones

Nokia Enterprise Solutions has released **Mail for Exchange (MfE) Client Version 2.0** for its E-series devices and for N73, N76, and N95 devices. The new version features a company directory that lets users perform Global Address List (GAL) searches. Users can also accept or decline meeting invitations and add meetings to their synchronized device calendar. E-series device users can search for content in MfE email synchronized to their phone. Supported servers include Microsoft Exchange Server 2007, Exchange Server 2003 SP1 and SP2, and Microsoft Small Business Server 2003 SP1 and R2. For more information, call 877-977-9199. A version of MfE 2.0 for North American AT&T customers was unavailable at press time, but T-Mobile customers can download the software at www.businesssoftware.nokia.com/mail_for_exchange_downloads.php.

Training

Learn About Microsoft Virtual Server 2005 R2



Written by Robert Larson, Janique Carbone and other members of the Microsoft virtual server team, the Virtual Server 2005 R2 Resource Kit provides tips and advice on administering the latest release of Virtual Server 2005. Published by Microsoft Press, the book includes detailed setup information for the Virtual Server COM API, provides a best practices virtualization project methodology, offers extensive troubleshooting advice, and covers other Microsoft and 3rd party applications that can help manage your virtual infrastructure. A companion DVD includes sample scripts, software and other resources. The Virtual Server 2005 R2 Resource Kit is available now and retails for $59.99. For more information, visit www.microsoft.com/mspress.

Exchange/Messaging

Increase Exchange Availability and Continuity

Teneros has unveiled **Application Continuity Appliance for Microsoft Exchange 2.0**, an updated version of their appliance that introduces Serial Attached SCSI (SAS) disk technology and support for 64-bit VMs. The appliance is available in two form factors: a 1U model supports 50-100 mailboxes, and a 3U model supports 250-2000 mailboxes. Both versions of the appliance have 8 GB of memory and 64-bit processors, allowing the appliance to run the Teneros Exchange Replication Engine and Microsoft Exchange in VMs. According to Teneros, the use of VMs enables updating and patching of the Exchange environment through a snapshot-based process hosted by Teneros. For more information, contact Teneros at 650-641-7400 or visit www.teneros.com.

SharePoint

Replicate SharePoint Content Among Sites

Syntergy Replicator for SharePoint integrates with Microsoft SharePoint technologies to provide multidirectional replication services among SharePoint servers. Replicator uses standard HTTP and HTTP Secure (HTTPS) protocols and data-compression technology to automatically update participating sites. The product supports geographically dispersed SharePoint users, provides custom views and content access to different users or groups, and is useful in failover situations and migrations from earlier versions of SharePoint. No client software is required. For pricing information or to view a demo, call 858-459-6356 or visit www.syntergy.com.

Storage

AMCC adds SAS Controllers to Product Line

Applied Micro Circuits Corporation (AMCC) recently announced availability of its **3ware 9690SA** Serial Attached SCSI (SAS) RAID controller. The SAS controller includes AMCC's unified RAID management interface and software suite. For configuration flexibility, the 3ware 9690SA offers three PCI Express low-profile controller choices: eight internal ports, eight external ports, or four internal/four external ports. The 3ware 9690SA is targeted at data center environments that require expanded connectivity and high levels of read and write performance, including databases, NAS, Web servers, cluster servers, supercomputing, nearline backup and archival, security systems, and professional audio- and video-editing appliances. For more information, contact AMCC at 800-840-6055 or visit www.amcc.com.

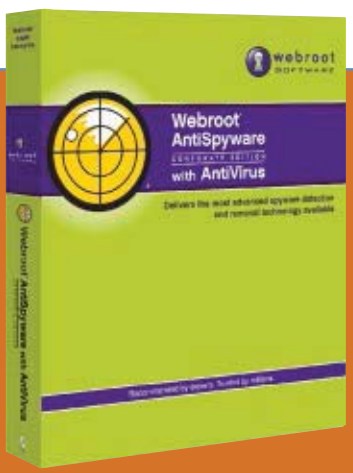
Storage

USB Combo Adapter for Hard Drive Configuration

Tripp Lite's new **USB 2.0 to SATA/IDE Combo Adapter** lets users connect computer hard drives to a Serial ATA (SATA) or IDE drive, turning the attached drive into an external USB 2.0 storage device. Data can be transferred from a hard drive to auxiliary drives or between auxiliary drives at speeds of up to 480Mbps. For more information, contact Tripp Lite at 773-869-1111 or visit www.tripplite.com.

Security

Corporate Virus and Spyware Protection



Webroot AntiSpyware Corporate Edition with AntiVirus 3.5 provides enterprises with protection against malware, spyware, and viruses. This latest version introduces Windows Vista compatibility, improved real-time threat detection, and enhanced reporting functionality. Other improved features include integration with Active Directory for ease of installation and enhanced detection of and protection from malware. Webroot Antispyware Corporate Edition with Antivirus 3.5 is now available and costs $28.26 per user for 1000-2500 seats. For more information, contact Webroot Software at 866-612-4268 or visit www.webroot.com.

Web Development

Web Application Performance Monitoring

Symphoniq has released **TrueView Express**, a web application performance monitoring system. The software allows IT pros to track and detect Web application performance problems that affect end-user productivity. The application offers customizable alerts that provide admins and site developers detailed information about Web infrastructure performance problems, then helps them isolate and diagnose causes of performance degradation. TrueView Express is $4,995, and can be downloaded from the Symphoniq Web site at www.symphoniq.com.

Hosted Services

Business Software on Demand

Verio Business Solutions provides a variety of popular applications in the form of hosted services for SMBs. Hosted versions of Microsoft Exchange 2007, McAfee Total Protection for Small Business, SugarCRM Professional, PC Data Backup, and Accrisoft Business Management and Productivity are available. All the applications are patched, managed and updated by Verio, and users pay a monthly fee for use of selected services. According to Verio, using the Software as a Service (SaaS) model reduces infrastructure overhead and minimizes IT support costs. For more information, contact Verio at 303-645-1900 or visit www.verio.com/saas.

InstantDoc ID 97589

Insights from the industry

How Do You Measure Computer Performance?

One of the most overlooked IT disciplines is that of computer measurement and testing. How can you compare different parts of your IT infrastructure if you're not using a sound testing methodology to ensure that you're comparing apples to apples?

Enter the Computer Measurement Group (CMG), a "not-for-profit, worldwide organization of data processing professionals committed to the measurement and management of computer systems." According to Director Dr. Michael Salsburg, CMG and its members are primarily concerned with evaluation of existing systems in an effort to maximize performance and optimize capacity management. "We currently have a strong interest in measuring server virtualization, and also in exploring the advantages of the ITIL standard," says Salsburg. "I think the adoption of ITIL really does have a payback for the organizations that adopt it."

CMG, Dr. Michael Salsburg

"We currently have a strong interest in measuring server virtualization, and also in exploring the advantages of the ITIL standard. I think ITIL really does have a payback for the organizations that adopt it."

—Dr. Michael Salsburg, CMG director

Another area that CMG is exploring is business performance management and how effective standards and measurement criteria can help define that segment of the IT infrastructure.

CMG holds annual conferences to discuss computer measurement and testing topics, such as load and stress testing, benchmarking, performance optimization, software performance engineering, resource management, capacity analysis, workload simulation, analytic modeling, and cost management. Salsburg maintains that the CMG conferences are a good fit for anyone who's responsible for acquiring computer equipment. Many participants have attended the event for years, which Salsburg attributes to the importance of computer measurement and testing to organizations. "Many [attendees] work at some of the world's largest IT infrastructures, places where performance testing and capacity planning are vitally important."

For more information about CMG and its conferences, visit www.cmg.org.

InstantDoc ID 97429

—Jeff James

Web-Filtering Appliances Add Services

Two Web-filtering appliances—Blue Coat Systems' Blue Coat ProxySG and St. Bernard Software's iPrism—recently added features in the form of Internet services. ProxySG's service adds a check for suspicious behavior to the URL-database check performed on the appliance; iPrism's service consolidates reporting for multiple appliances.

According to Chris King, Blue Coat director of strategic marketing, keeping a database of malicious URLs up-to-date is increasingly hard to do. To outsmart Web filters' databases of known-bad URLs, criminals are leaving their phishing Web sites up for only 24 hours, then taking them down and setting up new ones at new addresses. Criminals are also using Secure Sockets Layer (SSL) encryption on their Web pages to make them look more legitimate and to foil Web filters.

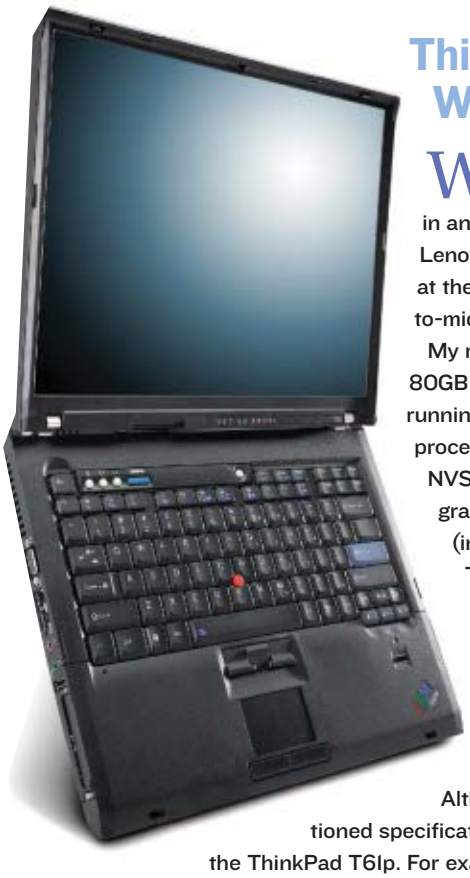
ProxySG's new service counters the Web-site churn by doing two checks when a user clicks a link in an email message. If the Web page isn't in the appliance's WebFilter database, the service sends the page to Blue Coat's data center, where proprietary algorithms analyze it for suspicious behavior, such as asking for identity information or downloading software. ProxySG can also analyze Web pages that use SSL encryption, because as a proxy, it terminates an SSL session and examines the traffic before re-establishing an SSL tunnel and sending the traffic on its way. After assessing a Web page, ProxySG categorizes it, warning the user and blocking the page if it's categorized as a phishing site.

St. Bernard added the Managed Enterprise Reporting Service to its iPrism appliances. Customers who run multiple iPrism appliances in various locations will be able to use the Internet-hosted reporting service to aggregate all their usage reports and archive them securely at St. Bernard's data center.

Andrew Lochart, St. Bernard VP of marketing and product management, described the reporting service as a "first step" in a new strategy to combine features of its LivePrism Web-filtering managed service with the iPrism appliance. Lochart pointed out that both deployment models have strengths and weaknesses. Appliances let customers control where the hardware is installed on the network, but they don't actually filter out the bad stuff before it hits your network, as services do. Appliances also have finite performance and bandwidth. St. Bernard's "hybrid" strategy will take these strengths and limitations into account when identifying the best place to perform a function (on the appliance or on the Internet) and will then implement the function accordingly.

InstantDoc ID 97421

—Renee Munshi



ThinkPad T61p Widescreen Laptop

When it comes to high-end business laptops, Lenovo has a long history of providing leading-edge features in an attractive, well-built package. Such is the case with the Lenovo **ThinkPad T61p**, an outstanding laptop that should be at the top of your list if you're looking for a laptop for a small-to-midsized business (SMB) or enterprise.

My review unit arrived with a 15.4" widescreen display, a 80GB hard disk drive, 2GB of RAM, a DVD-RW drive, and was running Windows Vista Business. A 2.2GHz Intel Core 2 Duo processor handles the processing duties, and a NVIDIA Quadro NVS 140M graphics controller with 128MB of RAM manages graphics and video. Integrated wireless communications (in the form of WiFi and Bluetooth) come standard on the ThinkPad T61p. A variety of processor speeds, RAM sizes, and hard disk drives are also available: The ThinkPad T61p can be configured with top-level components, including a 2.4GHz CPU, 4GB of RAM, and a 160GB 5400rpm Serial ATA (SATA) hard disk drive with full disc encryption. A variety of Vista versions are also available, including Vista Business 64.

Although many laptops are available with the aforementioned specifications, Lenovo also included some unique features in the ThinkPad T61p. For example, my test unit came with an integrated fingerprint reader for additional security. A shock-mounted hard disk drive helps prevent data from getting scrambled if the laptop is dropped, while an integrated roll cage provides extra protection and rigidity to safeguard the laptop's internal components from damage. Lenovo even engineered a drainage hole that channels fluids that get spilled onto the keyboard away from the laptop's internal components—Lenovo's public relations staff will be happy to know that I didn't get the chance to test that feature.

Setting up the laptop was easy and straightforward, and the pricing is competitive with comparable laptops. The ThinkPad T61p is a large laptop, but weighs just 6.5 pounds. According to Lenovo, the ThinkPad T61p's six-cell Lithium-ion battery will last up to 5.5 hours, while the nine-cell Li-ion battery will last up to 8.3 hours. My test laptop generated only a 4.0 (out of 5.9) on the Windows Experience Index because of a low graphics performance score. Upgrading to a more powerful NVIDIA graphics controller would raise that score. I've never been a fan of the pencil eraser-sized TrackPoint device; however, Lenovo thoughtfully includes a traditional touchpad as an alternate mouse control method. One thing I didn't like about the ThinkPad T61p is that some of the buttons at the top of the keyboard seemed a bit narrow, but I digress. There really isn't much not to like about this laptop, which is clearly one of the best business laptops currently available. If your IT shopping list includes laptops, take my advice and give the ThinkPad T61p a look.

InstantDoc ID 97505

—Jeff James

SUMMARY

ThinkPad T61p Widescreen Laptop

PROS: Excellent performance; integrated security features; crisp and clear display; potent CPU

CONS: Small volume control buttons; modest graphics performance

RATING: ◆◆◆◆◆

PRICE: Starts at $1,369

RECOMMENDATION: If you're shopping for a laptop for a SMB or enterprise, take a look at the ThinkPad t61p—you'll be hard-pressed to find a better high-end business laptop.

CONTACT: Lenovo • 866-968-4465 • www.lenovo.com

Paul's Picks

Summaries of in-depth product reviews on Paul Thurrott's SuperSite for Windows

www.winsupersite.com

HP MediaSmart Server

PROS: Truly innovative storage platform; excellent backup and sharing capabilities

CONS: No domain support or integration with small business solutions

RATING: ◆◆◆◆◇

RECOMMENDATION: Although HP's entry into the Windows Home Server market can hardly be called an enterprise-class solution, it should prove popular with IT pros in their own homes and with small businesses looking for a simple and effectively centralized backup system. The **HP MediaSmart Server**, preinstalled with the Windows Home Server OS, is innovative on many levels, from the compact form factor with hot-swap Serial ATA storage to the streamlined setup process that guides you past Microsoft's confusing defaults. MediaSmart Server is the best home server I've seen so far.

CONTACT: Microsoft • 800-426-9400 • www.microsoft.com

DISCUSSION: www.winsupersite.com/reviews/whs_hp.asp

Ultra-Mobile PC

PROS: Compatible with most Windows software; portable

CONS: Underpowered hardware; small screen; lack of integrated keyboards

RATING: ◆◆◆◇◇

RECOMMENDATION: I desperately wanted to like the **Ultra-Mobile PC**, created by companies such as OQO and Samsung to Microsoft specifications. But the devices are too slow and too limited to take the place of a real mobile computer. Microsoft's ultra-mobile software solutions are quite nice. If the hardware catches up—which it could with the debut of a new Intel chipset in early 2008—then the Ultra-Mobile PC could be just what the mobile professional ordered.

CONTACT: Microsoft • 800-426-9400 • www.microsoft.com

DISCUSSION: www.winsupersite.com/reviews/winvista_origami.asp

InstantDoc ID 97578

CONTINUOUS DATA PROTECTION

Find the best data recovery product to fit your needs

BY JOHN GREEN

[**Editor's Note:** Following is a summarized version of John Green's CDP comparative review. To read the full-length version of the article, go to www.windowsitpro.com and enter InstantDoc ID 97601.]

The term *continuous data protection* (CDP) has a variety of meanings. To some, CDP means an ability to back up changed data at regular intervals. Broader definitions include network and server protection. For the purpose of this article, I'm defining *true* CDP as the ability to recognize changes to data at an application's transaction level, as well as the ability to recover the state of the data to the point in time represented by the completion of any transaction.

Although many products are marketed as CDP solutions, I was able to consider only a few for this review. I narrowed the field by looking for products that offer support for two of Microsoft's key applications: SQL Server and Exchange Server. I focused my testing on SQL Server support.

During testing, I found that CDP's real value proposition is in a product's ability to go beyond simply providing continuous backup—to also use CDP to support larger objectives. A common thread among the four products I ultimately reviewed is their ability to maintain copies of protected data both locally and at a remote location in support of disaster recovery scenarios. Beyond that, the four products have more differences than similarities.

CA XOsoft WANSyncHA

CA XOsoft WANSyncHA incorporates CDP technology into an application server high availability product. The CDP portion of WANSyncHA is intended to bridge the protection gap between snapshots. By relying on the existing known good application data states provided by traditional backup and snapshot technologies, WANSyncHA minimizes the disk space required for the transaction-oriented rewind data. As a high availability product, WANSyncHA maintains a usable replica of the protected application server and can quickly fail over to the replica when necessary. A key application feature called Assured Recovery simplifies periodic testing of the failover process, including a rollback of test transactions applied to the replica during testing.

WANSyncHA has two installable components: the XOsoft engine, which runs on every server participating as a master or a replica; and the management console, WANSync Manager, which you can install on any Windows workstation or server. In a SQL Server environment, both the master server and the replica server must have the same configuration—both must be running the same service pack and hotfix level, as well as have the same storage configuration for protected databases. The management console, if you plan to use the remote installation facility, must run Microsoft .NET Framework 2.0.

The XOsoft engine, running as a service on each participating server, is WANSyncHA's interface to each supported application—Microsoft IIS, Exchange, SQL Server, Oracle, and NTFS, including 64-bit versions of supported applications. You can use the WANSync Manager to create WANSync scenarios that control what

SUMMARY

Windows IT Pro EDITOR'S CHOICE

CA XOsoft WANSyncHA 4.0.72

PROS: Maintains a remote server replica and supports automatic failover; leverages snapshot and traditional backup data to minimize the transaction-oriented storage requirements; Assured Recovery simplifies periodic testing of recovery procedures; data rewind operations work quickly for point-in-time recovery

CONS: Switching back after a failover caused by loss of the primary server requires a full replication of data back to the original primary server

RATING: ◆◆◆◆◆

PRICE: $2,000 to $7,200 per server, depending on the server's OS (Virtual Machine, Standard, Enterprise, Cluster) and applications to be protected (files, SQL Server, Exchange)

RECOMMENDATION: When you need true CDP with rapid remote application recovery, look at WANSyncHA first.

CONTACT: CA • 800-225-5224 • www.ca.com/us

the engine does. The wizard-driven process is easy to complete. After I selected a SQL Server high availability scenario, the wizard had me select master and replica SQL Server machines and then displayed the SQL Server instances and databases it found on the master server. I selected check boxes to indicate the databases I wanted to protect. Next, the wizard displayed the directories holding the database files that WANSyncHA would replicate. A properties page provides options to tailor WANSyncHA's behavior on the master and replica servers. By default, CDP—the data rewind capability—is turned off, so I enabled it and configured the maximum disk space utilization. The next screen displays default switchover properties, including the method WANSyncHA will use to redirect network traffic to the replica server. The default is to redirect the application's DNS name to the replica's IP address. You can configure switchover to occur automatically when WANSyncHA detects failure of the master, or manually. Similarly, you can configure replication back to the master after switchover to start automatically or manually. WANSyncHA caches updates locally when the destination server is unavailable, and sends the data when communication is restored. WANSyncHA will use the Assured Recovery feature to schedule integrity testing to run periodically, or let you trigger it manually. By default, Assured Recovery performs only basic testing (i.e., connecting to the database). You can script more complex testing to meet your needs. Near the end of the scenario creation wizard, WANSyncHA runs more than 100 proactive configuration checks to help prevent unexpected problems later. When complete, the wizard offers the option to run the scenario—performing initial replication and beginning data protection. I selected this option, and when initial replication completed, WANSyncHA produced an HTML report detailing the data sets that were replicated.

> WANSyncHA maintains a usable replica of the protected application server and can quickly fail over to the replica when necessary.

I was impressed with WANSyncHA's operation. Although it doesn't perform the rapid failover you'd see in a server cluster—which you shouldn't expect in a product such as this—it performed very well in my tests. Administrators will appreciate the ability to tailor the product to meet their needs, both in configuring switchover and in customizing the Assured Recovery features to fully test the recovery procedures in various environments. The data rewind feature is easy to use and gives you plenty of flexibility (enough, but not too much) to retain rewind data to meet your applications' needs.

SonicWALL CDP 4440i

SonicWALL's CDP appliances provide real-time backup for permanently and intermittently connected Windows systems. I tested the **SonicWALL CDP 4440i**, the largest of SonicWALL's four CDP appliance models; its Enterprise Manager reported about 550GB of storage capacity. All the models have a single enabled Ethernet connection. The 3440i and 4440i support Gigabit Ethernet and include a second, currently unusable network interface. SonicWALL offers several optional features and services, including Site-to-Site Backup, an Offsite Data Backup Service, Bare Metal Recovery for servers and workstations, and ongoing support services and software updates.

When I selected the SonicWALL CDP appliance for review, I was under the impression that it supported true CDP for SQL Server machines—that is, a transaction-oriented backup allowing any-point-in-time restore. In fact, CDP supports recovery to the level of an individual transaction log backup, which the SonicWALL CDP device lets administrators schedule as frequently as every 30 minutes.

I used the 4440i's Web interface to configure the appliance for my network. I downloaded the current SonicWALL CDP software package and installed it on the Windows XP system I wanted to use as the management console. The software package installed the CDP Agent, which is the key client-based component. The agent explores the local system for supported applications and monitors selected applications and directories (the ones you configure) for changes to data, sending new and changed data blocks to a CDP device. The software package also installed two user interfaces. The CDP Enterprise Manager is used to configure reporting, alarms, and data recovery, as well as policies for use with agent systems. The CDP Agent Tool provides users on protected systems (those with the agent installed and configured) with an interface they can use to configure and monitor local CDP operations and to recover file versions. The Enterprise Manager is always installed along with the agent on protected systems. I used the Enterprise Manager to configure basic administrative settings, including the password that protects access to the 4440i's configuration.

SUMMARY

SonicWALL CDP 3.0 on the SonicWALL CDP 4440i Appliance

PROS: Easy to implement data protection appliance for SQL Server, Exchange, AD, and NTFS files; optional features support automatic offsite replication of protected data; CDP 3.0 makes recovery to a previous state simple, with automatic selection of the correct set of backup files

CONS: Rather than supporting true transaction-aware CDP for SQL Server, SonicWALL's CDP 3.0 recovers to the state contained in a log backup, which you can configure the SonicWALL appliance to capture as frequently as every 30 minutes; incomplete support to configure protection for a system remotely—alternatives include local configuration or use of a remote desktop product

RATING: ◆◆◆◆◇

PRICE: $7,999 to purchase; support contracts start at $1,679 for one year of 5 × 8 support with software updates

RECOMMENDATION: Take a look at SonicWALL's CDP line if the 4440i's storage capacity and the 30-minute recovery point meet your needs, and if you can live with local or remote desktop access to configure protected systems.

CONTACT: SonicWALL • 888-557-6642 • www.sonicwall.com/us

Enterprise Manager also lets you create agent policies in which you can specify a disk quota for the agent, default folders and applications to protect, and backup exclusions at the file extension level. The policy feature doesn't seem to be fully developed; it presented only Outlook and Outlook Express as the application options and didn't give me an option to configure SQL Server-related or Exchange-related policies. Nor did it allow browsing either local or remote root (e.g., C$) drive shares to assist the creation of file backup policies. Because policies are the only tool that allows remote management of CDP devices' backup configuration, a more complete policy feature would be extremely useful. Instead, administrators must use the Agent Tool installed on a computer to configure protection for that system. Remote configuration is possible using a remote desktop application.

I used the Agent Tool to designate a directory on my XP console for protection. The agent immediately backed up the directory to the 4440i. As I altered files in that directory, I was able to display and restore previous versions of a file to any location, including the original. This method for creating secure file version backups for local users is both easy and effective. Note that CDP supports protection of local disks but not remote file shares.

Because I was testing recovery in a SQL Server environment, I installed the agent on a SQL Server 2005 system with several active databases. The agent uses the standard SQL Server API to perform full, differential, and log backups, so CDP won't create log backups for databases set to the simple recovery model.

The facilities for protecting and restoring SQL Server databases are easy to use, with few options. After installing the agent and tools to a SQL Server 2005 system, I was able to quickly configure protection for several databases. For each database I was able to specify the backup interval for full, differential, and log backups, which default to monthly, weekly, and every two hours, respectively. CDP retains two full backup files, as well as associated differential and log backups. Recovery of a SQL Server database is similarly simple.

Overall, SonicWALL's CDP 3.0 and the 4440i appliance were very easy to implement and use. Although CDP 3.0 doesn't meet my definition of true CDP in its support for SQL Server, it will meet many organizations' Recovery Point Objectives (RPOs).

DPM 2007

DPM 2007 is the latest enhancement to Microsoft's near-CDP application and system recovery suite. The product has specific support for a variety of Volume Shadow Copy Service (VSS)-supporting applications. DPM also supports protection of XP- and Windows Vista-based (except Home editions) shares.

DPM runs on a Windows Server 2003 or Windows Storage Server 2003-based system, where it maintains replicas of protected data. A DPM agent runs on all protected systems and copies protected data to the DPM server at user-specified times or intervals in two ways: using what DPM calls an Express Full Backup, to create a full recovery point, and using what DPM calls Synchronization, to create an incremental backup. Express Full Backup uses a data block-oriented copy to create a replica of the protected object (e.g., a database, Exchange storage group, or Virtual Hard Disk—VHD) on one of DPM's storage disks. The agent tracks new and changed data blocks within protected objects on the volume and sends only those blocks to the DPM server when subsequent Express Full Backups are run. Synchronization, the creation of incremental recovery points, is available only when the protected application supports incremental backup. In the case of SQL Server, DPM lets you specify a Synchronization frequency only when the protected database maintains a transaction log file. For simple recovery model databases, only Express Full Backups create a recovery point. The DPM agent makes use of the VSS writer's ability to quiesce application activity and produce a snapshot of the data object in a stable, usable state. Once the data is preserved at the DPM server, the agent deletes the snapshot, freeing its storage. Similarly, when recreating a Full Express Backup replica after an outage, the agent compares the blocks of the existing replica on the DPM server to a snapshot of the current data object on the protected system and sends only the differences. You can schedule Express Full Backups to occur as frequently as every 30 minutes by selecting the days of the week and the times of day DPM will perform the backup. You schedule Synchronization by selecting an interval of as little as 15 minutes. Although the incremental backup provided by Synchronization lets you recover changes that occur after the prior Express Full Backup, recovery is often faster using a recent Express Full Backup, with fewer incremental recovery points (i.e., log backups) to apply.

Microsoft provides two user interfaces: the DPM Administrator Console, which is DPM's primary management GUI; and the Management Shell, a command-line interface that supports scripted operations. DPM stores protected data within its storage pool, which consists of one or more physical disks dedicated to DPM. After installing DPM, adding at least one physical disk to the storage pool is the first configuration task. DPM allocates volumes on storage pool disks for each protected data object where it stores replicas and Synchronization recovery points, extending volumes when necessary.

I discovered one inconvenient feature. I choose to modify a protection group, adding two file directories comprising about 20MB of data. Even though my storage pool had more than 13GB of available space, the Administrator Console reported insufficient space for the protection group. After I freed more space by deleting a protection group, DPM allocated 15GB of disk space for the 20MB of file data. I suspect that in circumstances like this—when your data structures' growth and change behavior doesn't match DPM's built-in assumptions—administrators would prefer to use DPM's support for custom storage volumes that let you, rather than DPM, manage the

SUMMARY

System Center Data Protection Manager 2007

PROS: Broad support for Microsoft applications, and third-party VSS-enabled applications with vendor support; designed for ease of use—all tasks are wizard driven and easy to complete; clean integration of both disk and tape into short- and long-term protection policies let you easily implement data retention and recovery for the full life cycle of your data

CONS: DPM's disk space allocation for storing protected data might not efficiently match your data's growth and change patterns; however, there's an option that lets you manage storage allocations yourself

RATING: ◆◆◆◆◇

PRICE: $573 per DPM server; $426 per Enterprise Server management license; $155 per Standard Server management license

RECOMMENDATION: DPM 2007 is a well-designed near-CDP product that I recommend to all users of the key Microsoft applications that it supports.

CONTACT: Microsoft • 800-642-7676 • www.microsoft.com

space allocations. DPM lets you specify a preallocated, custom storage volume only when you add a member to a protection group.

Overall I found DPM to be very easy to use. Its integration of disk and tape technology let you easily implement DPM as an extension or evolution of existing backup and recovery procedures. Administrators will most appreciate the recovery features' simplicity and flexibility. When you want to simplify managing your backup data, simplify recovery, or create a working copy of application data for another use, DPM is an easy choice.

TimeData

TimeSpring's **TimeData** is a CDP solution for protecting files, Exchange data, and SQL Server databases. TimeData is a true CDP solution, allowing recovery to any point in time.

TimeData comprises several components. The key system is TimeData's repository server, where TimeData stores protected data. TimeData stores protected data in its Event Log file and installs an instance of SQL Server 2005 (provided with a limited-use license) that TimeData uses to index the data in the Event Log file. To enhance performance, both the Event Log file and the TimeData database should be on separate disks, with system and paging files on other disks. The Event Log disk should be six to eight times the size of the data you're protecting. TimeSpring recommends use of a separate, dedicated network for the transfer of data from protected servers to the repository server.

SUMMARY

TimeData 2.7.1

PROS: Easy to implement and manage—the Management Console allows effective centralized configuration and management of all protected systems; architecture is very flexible and seems highly scalable; transaction-level recovery even for simple recovery model databases; includes tools for message-level restore when licensed for Exchange

CONS: Relatively heavy system memory and storage resource requirements; lacks integrated tools for recovery of protected applications—TimeData provides the point-in-time data, and you employ standard tools to use the data

RATING: ◆◆◆◆◇

PRICE: Per server pricing: NTFS $1,295; SQL Server $3,995; Exchange starting at $3,995

RECOMMENDATION: Use TimeData if its custom recovery methods fit your environment.

CONTACT: TimeSpring Software • 888-375-7634 • www.timespring.com

You install the TimeData Agent on servers whose data you want to protect—which TimeSpring calls Data Servers. The agent queues data on its way to the repository using an Event Cache, which for performance reasons should be on its own disk on each data server. You use the TimeSpring Management Console on the repository server to configure and manage TimeData. Remote management is possible only with the use of a remote desktop application.

After installing the software, the next step is to create a content group—a named collection of files and data structures on a single data server that you want TimeData to protect. To give you some control over the granularity of potential restore points with SQL Server, TimeData lets you configure when it will create a new version, which is what TimeData calls a potential restore point.

For additional flexibility, including offsite backup, TimeData lets you configure a data server with more than one repository. Using the second repository server, you can import existing content groups from the data server, or create new content groups. Allowing different content groups from a single server to connect to different repositories lets you be selective about the data that occupies a WAN link, and lets you distribute the protection of large, active data servers between several repositories.

TimeData provides a lot of flexibility for recovering data. You start by using the TimeSpring Management Console to display and select a version of the database to work with. The console will display as many as 1,000 timestamped versions at a time, and it lets you filter by time range to help locate the desired version. After selecting a version to work with, you create a fixed time retrieval view of the content group, which TimeData adds to the console tree. Within the console, you can select a database from the view and have TimeData write it to another location on disk. TimeData also presents the files on the TimeData drive, a virtual disk drive on the repository server mapped by TimeData to a drive letter you specify at installation time. TimeData creates the virtual drive with a network share, letting you access the files across the network.

Overall I found TimeData easy to install, configure, and use to retrieve point-in-time versions of data files. The fixed time retrieval view and the TimeData drive provide rapid access to point-in-time data across a network share. I discovered a limitation to the usefulness of the TimeData drive share when the number of characters in the path to a SQL Server MDF file was too long for remote access—I had to create a new share at the folder that contained the files I wanted to copy. TimeData's ease of use ends with rapid access to the file. It lacks features to recover production databases to a point in time, leaving it up to you to use standard SQL Server database tools to work with the point-in-time database. On the plus side, its architecture seems well suited to a highly scalable implementation.

Best of the Best

Each of these four products will find its niche. In the end, I selected my Editor's Choice by looking at how well each product fulfilled on the promise of it features. My Editor's Choice goes to CA XOsoft WANSyncHA for its ease of use, for its effective failover and failback feature set, and for the balance it strikes between effective data protection and system resource requirements.

InstantDoc ID 97601

John Green
(john@nereus.cc) is president of Nereus Computer Consulting.

Learning Path

WINDOWS IT PRO RESOURCES

"Continuous Data Protection," InstantDoc ID 95794

"Data Protection for Windows Server Workloads," InstantDoc ID 97500

"System Center Data Protection Manager 2007," InstantDoc ID 95981

"What you need to know about Microsoft System Center Data Protection Manager," InstantDoc ID 48116

WHITE PAPER

"The Essential Guide to Continuous Data Protection for Exchange"
www.windowsitpro.com/essential/index.cfm?fuseaction=show&guid=a491c9d7-bc17-4591-a3c4-e6c629ce0ac8

iSCSI SANs for SMBs

Check out these affordable, high-performance network storage solutions

Over the past few years, network storage product prices have dropped dramatically as performance and storage drive capacities have increased. Part of this growth is attributed to the continued success of the iSCSI storage protocol, which has been making inroads in the network storage market. According to IDC, the iSCSI SAN market is projected to top $5 billion by 2010.

Several factors are driving the growth in the adoption of iSCSI SANs, ranging from increased use of virtualization in the data center to a greater reliance on data-driven business environments that employ storage-hungry applications such as business intelligence (BI) and massive database applications. Hardware costs have also plummeted over the last few years, making enormous amounts of disk storage available for a fraction of what they formerly cost.

Because of those factors, a flood of high-performance, low-cost iSCSI SAN products are now available for small-to-midsized businesses (SMBs). Our buyer's guide can help you choose the right iSCSI SAN for your organization. Affordability is an important factor for SMBs, so none of the products listed in this buyer's guide exceeds $15,000.

Why Implement an iSCSI SAN?

What are the benefits of moving from DAS to an iSCSI SAN? DAS tends to be more difficult to manage as your IT infrastructure grows because it requires that local storage for each server be administered separately. DAS also doesn't allow for common storage in a heterogeneous infrastructure, such as in environments that might have clients running Mac OS X or Linux in addition to Windows.

Until just a few years ago, the only way to realize the benefits of a SAN was to purchase a Fibre-Channel (FC) SAN. However, the high implementation and support costs of FC SANs kept most SMBs from implementing them. That all changed with the introduction of iSCSI SANs.

Like FC SANs, iSCSI SANs consolidate storage for multiple servers into one manageable resource. iSCSI SANs benefit from the simplicity and ubiquity of the Ethernet and iSCSI protocols, as well as the continuing drop in fixed-disk prices. When combined with network storage applications, such as Windows Storage Server 2003, iSCSI SANs emerge as viable network storage solutions for nearly all SMBs.

Things to Keep in Mind When Purchasing an iSCSI SAN

According to Joel Reich, general manager of NetApp's SAN/iSAN business unit, purchasing an iSCSI SAN can be a straightforward process if you're armed with the correct information. It's important to do some extensive research to find a solution to meet your storage needs and important to decide how your iSCSI SAN will be deployed.

Cover as much of your organization as possible. When it comes to buying storage, Reich suggests that you try to find an iSCSI SAN that will cover as much of your infrastructure as possible. Remember, only the parts of your infrastructure that have access to your iSCSI SAN will realize the benefits of having a speedy, redundant SAN.

Shop for scalability. Although buying adequate amounts of storage for your current situation is important, Reich explains that you don't necessarily need to follow the conventional wisdom that advises administrators to "buy as much storage as you can afford." Choosing an iSCSI SAN that's scalable enough to respond to the growing needs of your business is a better approach, according to Reich. "The system you choose should allow you to easily add capacity and performance over time. Not all businesses have million-dollar IT budgets … it's important to have a system that allows you to pay as you grow."

Leverage your Microsoft investment. Reich says that Microsoft has helped drive the adoption of SAN storage options, including iSCSI SANs, with applications such as SQL Server and Exchange that use block storage protocols. iSCSI is a block storage protocol, but NAS doesn't support block storage. Given the proven interoperability between Windows applications and iSCSI, Reich says that businesses running many Windows applications will find iSCSI SAN storage to work well with their existing infrastructure.

Buy for the Future

Choosing and deploying an iSCSI SAN that can easily be expanded to accommodate your future needs and requirements is important. For example, is reducing power consumption (and related energy costs) a growing concern for your business? If so, choose an iSCSI SAN with a large-capacity drive, which tends to provide a more efficient watts-per-terabyte power-consumption ratio. If network performance is important, look for an iSCSI SAN that includes support for the upcoming (and much faster) 10Gbps Ethernet standard. And if the ability to easily add storage in the future is at the top of your must-have list, be sure to look for an iSCSI SAN that lets you easily hot-add and hot-swap new disk storage. When armed with the right information and the best iSCSI SAN for your specific environment, you can enjoy the affordable benefits of NAS storage for years to come.

InstantDoc ID 97607

Jeff James (jjames@windowsitpro.com) is senior editor, products, for *Windows IT Pro* and *SQL Server Magazine*. He specializes in virtualization and terminal services and has over 15 years of experience as a writer and digital-content producer.

EDITOR'S NOTE

The Buyer's Guide presents vendor-submitted information. To find out about future Buyer's Guide topics or to learn how to include your product in an upcoming Buyer's Guide, go to www.windowsitpro.com/buyersguide.

Company	Product	Price	Disk Capacity: Base	Disk Capacity: Total	Fibre-Channel Support?	Data Replication Support?	Data Snapshot Support?	Volume Shadow Copy Service (VSS) Support?	Management Software?
Celeros 650-216-7900 www.celeros.com	Celeros Windows Unified Storage Server	$7,500 for 12TB	12TB	76TB	No	Yes	Yes	Yes	Yes
Dot Hill Systems 760-931-5500 www.dothill.com	Dot Hill 2330	$11,864 for 3TB SATA	3TB SATA/ 876GB SAS	42TB SATA/ 16.8TB SAS	No	No	Yes	No	Yes
Hitachi Data Systems 408-970-1000 www.hds.com	Simple Modular Storage 100	$5,000 – $15,000	520GB+	9TB	Yes (in early 2008)	Yes	Yes	Yes	Yes
HP 800-888-9909 www.hp.com	HP StorageWorks 400 All-in-One Storage System (Ai0400)	$5,499 for 1TB SATA	4 drives: 1TB SATA	10TB	No	Yes	Yes	Yes	Yes
	HP StorageWorks 600 All-in-One Storage System (Ai0600)	$7,159 for 1.5TB SATA; $9,949 for 860TB SAS	6 drives: 1.5 TB SATA or 860TB SAS	72TB	No	Yes	Yes	Yes	Yes
	HP StorageWorks 1200 All-in-One Storage System (Ai01200)	$8,759 for 3TB SATA; $13,899 for 1.7TB SAS	12 drives: 3TB SATA or 1.7TB SAS	81TB	No	Yes	Yes	Yes	Yes
Intransa 408-678-8600 www.intransa.com	Intransa EdgeBlock/ StorStac BuildingBlock	$1,795/TB (EdgeBlock); $2,000/TB (StorStac BuildingBlock)	3.75TB	1,000TB	No	Yes	Yes	Yes	Yes
LeftHand Networks 303-217-9000 www.lefthandnetworks.com	NSM 2060	$15,000	3TB	3TB	No	Yes	Yes	Yes	Yes
StoreVault/NetApp 877-278-7858 www.storevault.com	StoreVault 5300	Starts at $3,000 for 1TB	4 drives 250GB or 1TB raw	8 drives 500GB or 4TB raw	No	Yes	Yes	Yes	Yes
Variel Technology 949-753-8881 www.variel.com	VIPN310X—3U Appliance Variel iSCSI Engine	$6,890 for 3TB; $8,975 for 12TB	3TB	12TB	No	Yes	Yes	Yes	Yes
	VIPN310X—3U Appliance Microsoft Windows Unified Data Storage Server 2003	$7,490 for 3TB; $9,175 for 12TB	3TB	12TB	Yes, includes optional host bus adapter	Yes	Yes	Yes	Yes

EDITOR'S NOTE: Some vendors that you might expect to see in this Buyer's Guide said they didn't have a product that exactly matched the criteria or didn't

	Data Protection Manager?	Remote Management Capability?	Hot-Swap Capability? Drives? Power Supplies?	Fault-Tolerance/ Redundancy Support?	Support for SATA Drives? SAS? Both?	Thin Provisioning?	Storage Pool?	Speed and Number of Network Interfaces?	Network Interface Teaming for Speed? Redundancy? Both?
	Yes	Yes	Yes / Yes / Yes	No	Both	No	Daisy chain SAS JBOD chassis	2 x I Gigabit Ethernet (GbE)	Both
	Yes	Yes	Yes / Yes / Yes	Yes	Both	No	Can be added with management software	IGB per port, 4 ports	Both
	Yes	Yes	Yes / Yes / No	Yes, dual controller models have no single point of failure, ships in RAID 6 (dual parity) configuration	Both	Yes	LUN concatenation; automigrate to larger models without disruption	4 x IGbE	Both
	Yes	Yes	Yes / Yes / No	Yes	SATA	No	Can be grown while applications are online	2 x IGbE included	Both
	Yes	Yes	Yes / Yes / Yes	Yes	Both	No	Can be grown while applications are online	2 x IGbE included (Supports additional IGbE or IO GbE ports)	Both
	Yes	Yes	Yes / Yes / Yes	Yes	Both	No	Can be grown while applications are online	2 x IGbE included (Supports additional IGbE or IO GbE ports)	Both
	Yes	Yes	Yes / Yes / Yes	Yes	SATA	Yes	With DynaStac thin provisioning (included)	I x GbE (8 x IGbE = 8GbE) IOGbE (4 x IOGbE = 40GbE)	Both
	Yes	Yes	Yes / Yes / Yes	Yes	SATA	Yes	Automatically	2 x IGbE	Both
	No	Yes	Yes / Yes / No	No	SATA	Yes	FlexVol or thin provisioning to add capacity	4 x IGbE	Both
	Yes	Yes	Yes / Yes / Yes	Yes, application-specific integrated circuit (ASIC) hardware RAID; redundant power supplies and fans	SATA	No	With Virtual Disk Service (VDS)	4 x IGbE	Both
	Yes	Yes	Yes / Yes / Yes	Yes, hardware RAID; redundant power supplies and fans	Both	No	With VDS	2 x IGbE	Both

respond to our requests for information about their products.

BY GUIDO GRILLENMEIER

AVOID ACTIVE DIRECTORY PAIN

Time synchronization, cross-forest authentication, least privilege model, and 64-bit

Over the past eight years I've helped plan, implement, and operate various Active Directory (AD) infrastructures. And as much as I value AD's power and strength, I've also learned quite a few annoying things about AD that sometimes prevent it from operating as smoothly as possible. In this article I discuss some of these annoyances and explain how to best work around them.

Special Hardware Problems

In general, all AD domains are rather tolerant to hardware problems that take down a single domain controller (DC). Of course this is only true if you follow the best practice of implementing more than one DC per domain and if you continuously monitor that they're replicating the changes amongst themselves. This way, if one DC fails for some reason, clients wanting to authenticate to the domain will leverage DNS to find another DC in the network to connect and authenticate to. For normal operations, no problems occur even if one of the special Flexible Single-Master Operation role-holder DCs goes down for a few hours or even a few days. AD is designed to operate without all the FSMO DCs being available all the time. Obviously, you shouldn't update your schema or mass-create new objects in your domain when specific FMSO DCs are down. But normal operations, such as users changing their passwords or administrators adding an occasional new object to the domain, will still run. This is one of the key strengths of AD and its multi-master replication model.

But sometimes it isn't the hardware failure of the DC that causes a problem. Sometimes problems don't start until you repair the hardware and reboot the DC—especially if the DC is your domain's PDC emulator. By default, all DCs in an AD domain synchronize their time with the PDC emulator of the respective domain. Computers and servers joined to the domain then synchronize their time with the DC they use for authentication—usually a DC within their AD site. For Kerberos authentication to work, all these clients and DCs must be synchronized in time. (In an AD domain, Windows 2000 Server and later clients and servers leverage Kerberos by default.) If the time skew (difference) is too large between a client and the server it wants to access a resource from, such as a file share, authentication to the resource server fails. The default accepted time skew in an AD forest is five minutes. So even if a user or computer properly authenticates to a domain, it might fail to access a server because of a time difference.

What does all of this have to do with the hardware failure of a DC in your domain, potentially even the PDC? Quite simple: If your hardware repair involves replacing a server's motherboard, you usually also replace the on-board clock. And it's highly unlikely that

ILLUSTRATIONS BY RYAN ETTER

the time set on the new motherboard's system clock is in sync with the rest of your AD forest. If you then just reboot the PDC while it's on the network, the other DCs will synchronize their times with the PDC when they see that it's online again. Thus, you might introduce a time skew on various machines in your environment that's unacceptable to Kerberos. Although your PDC might have been properly configured to replicate with an external time source, the wrong time has now made its way into your network and will cause problems such as Microsoft Exchange Server servers not being able to leverage Global Catalogs (GCs) in their site for LDAP lookups, or users not being able to access file shares. Your environment might not normalize for hours or days and might even require manual intervention.

The solution to this problem is as simple as the problem itself: If you need to replace a DC's motherboard, particularly for a broken DC that hosts the PDC emulator FSMO role, remove the network cable before you reboot the DC. After the DC reboots successfully (which might take longer than normal because the DC won't be able to find other DCs to replicate with), you need to log on locally and update the time on the DC. Afterwards, you can plug the network cable back in. Alternatively, if your PDC is still responsive, you can temporarily transfer the PDC role to another DC and transfer it back after replacing the motherboard. These methods prevent time-synchronization problems that in turn cause trouble with network authentication.

Cross-Forest Authentication

It's difficult enough for most AD administrators to understand how clients leverage DNS to locate DCs of their own forest or domain within their own network. So before we look at how this process might work across different AD forests and networks, let's quickly review the DC location process within an AD domain.

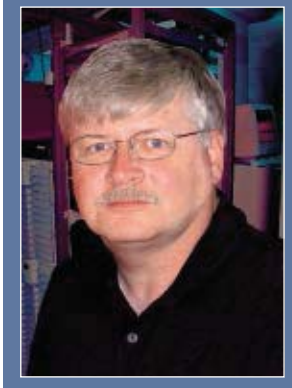
In short, a Win2K or later client that has never authenticated to an AD domain will query DNS to ask for any DC that's responsible for its own domain. The client does so by asking the DNS server to return the list of all DCs that have registered the generic DC locator record (which by default includes all DCs in an AD domain). To retrieve these records, the clients first query for the generic LDAP service records in the DNS hierarchy's _msdcs zone. For an AD domain called MyCompany.net, these generic records are located in the following DNS hierarchy: _ldap._tcp.dc._msdcs .MyCompany.net.

The client then contacts a few of the DCs in the list returned from the DNS server, notifies them of its intention to be authenticated, and waits for the first DC to respond. However, the DCs are smart enough to understand the situation and therefore check the IP address that the client is using in its request. They see that the client is joined to the domain, and they compare the client's IP address with the site

IT Pro Hero

Castaway on Command-Prompt Island

BY CURT SPANBURGH



A Windows admin finds a lifesaver in the SC command-line tool to help him get a crucial server back online

As a computer consultant, I often encounter system administrators who find themselves in trouble if they can't perform an action through the GUI. With many good command-line tools available, and resources such as *Windows IT Pro* to learn about them, admins should have a variety of methods in their toolbox to solve problems.

Here, for instance, is the story of a Windows administrator—we'll call him Frank. He relied mostly on the Windows GUI administrative tools to perform systems management tasks. However, one day when Frank couldn't access a crucial server in his company's data center, he had to find a command-line alternative to solve the problem. Here's what happened.

RPC Server Lost at Sea

On a certain Patch Tuesday, Frank had servers to patch at a data center. It was easier for him to apply the patches from a remote connection, so at around 9 P.M. he logged on to the system and patched all the servers, including the domain controller (DC) with the Global Catalog (GC) role.

After he rebooted everything, the servers all responded to a Ping. But when he tried to check his email, Microsoft Office Outlook couldn't find the Exchange server. Then he tried logging on to the DC but received an error message: *The system cannot log you on due to the following error: The RPC server is unavailable.* The good ship GUI was heaving and swaying in the waves, with no access to the GC role. Without this role running on an Active Directory DC, Exchange can't run.

Frank was desperate to find out what was going on with the server, and he remembered that he could use a Microsoft Management Console (MMC) snap-in to read the logs of another server. So he logged on to a member server to try running the snap-in but still couldn't reach

and subnet data stored in the AD configuration partition. With this data, the DCs determine the client's proper site, and they tell the client to connect back to the DNS server and query for the actual DC to authenticate to in its own site. The client then requests the proper Kerberos service record.

Let's assume the client is located in a branch office of the MyCompany.net AD domain and the AD site name is BranchSite. The client would query DNS for the site-specific Kerberos service records registered for this site. These records are located in the following DNS hierarchy: _kerberos._tcp.BranchSite._sites.dc._msdcs.MyCompany.net. Figure 1 also shows this hierarchy, from the Microsoft Management Console (MMC) DNS snap-in.

The DNS server will then return only DCs that are responsible for the client's site, which the client in turn leverages to authenticate to the domain. Fortunately, the client stores the information for the last AD site it belonged to in the registry and leverages this information directly the next time it needs to locate a DC. To find the AD site name that a client cached for itself, go to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\DynamicSiteName registry subkey.

Even after a user authenticates to his or her proper domain, cross-domain resource access involves a few more steps in multi-domain forests. Part of the DC locator process is repeated when the user accesses resources in another domain in the forest. Although all the domains in a forest trust one another, the Kerberos Ticket Granting Ticket (TGT) that the client received from its own DC at logon is valid only for requesting service tickets that in turn grant access to resources in the client's own domain. When a user accesses a resource in another domain in the same forest (e.g., a file server), the client again first queries DNS to locate a DC of the file server's domain to request a TGT that's valid in this domain. The good thing is that the client will immediately find the correct DC to use. Because the client already knows what site it's in, it uses a site-specific DNS query (such as the one I described) to locate a DC of the other domain.

One reason this process works so efficiently within a forest without the need to query for the generic DC locator records of the other domain is that all domains in the same forest replicate and use the same AD configuration partition. This partition also contains the site and subnet information, so that DCs from any domains in the forest properly register locator records for the respective AD sites. If no DC exists in an AD site, or if a site doesn't have a DC for every domain in the forest, the AutoSiteCoverage mechanism ensures that the closest DC will register a locator record in DNS. This means that within its forest, a client can always locate a site-specific DC for any domain in the forest. The client doesn't have to leverage the generic DC locator records, which might direct the client to a DC on the other side of the world to authenticate with. However, remember that this process assumes that the site-specific DCs are available—if not, the client will fail back to leveraging the generic DC locator records and might therefore experience slow authentication and GPO processing.

Suppose that you've just acquired another company that has its own AD forest. To efficiently allow collaboration between the employees of both companies, you decide to establish a trust across both forests. Your plan might be to later consolidate both forests; however, a forest trust is often the first step to allow

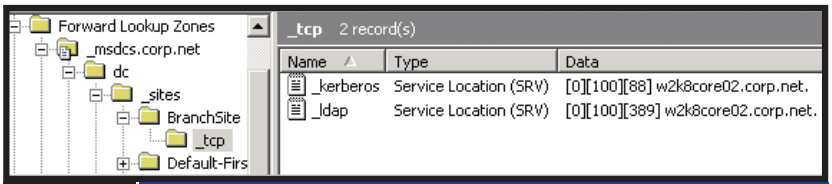


Figure 1: Site-specific DC locator records

IT Pro Hero

the DC. Frank had run aground on an uncharted island, unable to reach the "mainland" of the DC, and he couldn't get any information from the system to help solve the problem.

As he paced around, trying to think of a way out of this situation, he tripped over a laptop bag that appeared as if washed up on the sand. Looking inside, he found an issue of *Windows IT Pro*. With no better ideas, he started paging through the magazine.

SC Tool to the Rescue

Suddenly, he saw an article about a command-prompt tool he hadn't been aware of: SC (sc.exe), a tool that could be used to manage services running on a local or remote machine. The article was "The All-Purpose Service Controller," November 2006, InstantDoc ID 93400. As Frank read the article, he thought, "This tool could help me out of my predicament."

He logged on to the member server again and entered the SC command in the command window to learn its syntax, which came back as

```
sc <server> [command] [service name] <option1> <option2>...
```

Frank soon realized this wasn't a one-use tool, but a Swiss Army knife that would return him to the GUI and restore email service. He knew the server wouldn't respond by machine name, but it had responded to a Ping. So he entered this command:

```
sc \\192.168.10.10 query
```

In an instant, all the server's services and their information scrolled down his screen. He needed to narrow down the query to a specific service. According to the connection error message, the remote procedure call (RPC) service wasn't available, so Frank entered the following command to see what was going on with RPC:

```
sc \\192.168.10.10 query RPC
```

The command returned an error message: *[SC] EnumQueryServices Status:OpenService FAILED 1060: The specified service does not exist as an installed service.*

From this error message, Frank deduced that the SC command didn't recognize the RPC service's display name (i.e., RPC), so he retried the command using RPC's service name, rpcss. This time, the command results showed him that the RPC service was running,

Change the insides, not the outsides.

There's a whole new way to VoIP. And you don't need a whole new infrastructure to get it. That's because now it isn't about ripping and replacing. It isn't even about hardware. It's about software. Keep your hardware—your PBX, gateways, even your phones. Move to VoIP with software. Software that integrates with Active Directory,® Microsoft® Office, Microsoft Exchange Server, and your PBX. Maximize your current PBX investment and make it part of your new software-based VoIP solution from Microsoft. It's really big change, without changing it all. Learn more at microsoft.com/voip

VoIP AS YOU ARE.

Your potential. Our passion.®

Microsoft®

access to resources in different forests for both parts of a merged company.

The annoying thing about cross-forest authentication is that the client frequently fails to locate the correct DC in a trusted forest and is instead authenticated by a random DC—often not the DC you prefer the client to use. The good news is that you can easily solve this problem.

Similar to the cross-domain DC location process that I already described, when a client accesses a resource across a forest trust, the client also queries the trusted forest's DNS servers for the correct DCs for authentication purposes. The key thing to understand here is that the client queries DNS again for the site-specific Kerberos service records. The client does so by combining the site name from its own domain (MyCompany.net) with the domain name of the trusted forest's domain (OtherCompany .net) and would thus query in the following DNS hierarchy: _kerberos._tcp.BranchSite._sites.dc._ msdcs.OtherCompany.net. If no such AD site exists in the trusted forest, which is highly likely for a forest designed by a different AD team, the DNS query fails and the client must request the generic DC locator records. The client might then be authenticated by DCs of the trusted forest that are less than ideal to use, which will effectively slow down the cross-forest access to data and applications.

To prevent this problem, simply ensure that you create AD sites with the same names in both forests. Consider these new sites to be "shadow" sites of the trusted forest. You don't need to add new IP subnets to these sites for this solution to work, nor do the shadow sites need to contain real DCs. Instead, create a dedicated site link between each "shadow-site-for-MyCompany" and the closest "real-site-of-OtherCompany" connecting the two sites. Make sure no other sites are joined to this site link and that the shadow sites themselves aren't joined to any other site links. Doing so will guarantee that the proper DC of the OtherCompany.net forest adds the required SRV records to the respective shadow site via AutoSiteCoverage. These shadow sites will now ensure that your clients leverage the correct and closest DCs for authentication when accessing resources across a forest trust.

Enhancing the Usability of the Least Privilege Model

As companies have become more sensitive to IT security, AD administrators have begun to use at least two accounts with different privileges: one account for logon to clients and to perform regular office tasks (this account doesn't have any administrative rights in AD) and another account with sufficient privileges in AD to perform administrative tasks such as user and group management. As is often the case, increasing security doesn't make the processes more user friendly for the end user. In this case the end user is the AD administrator. Handling multiple accounts can be a hassle even when using the different OS features, such as right-clicking the MMC Active Directory Users and Computers snap-in and selecting *Run as* to start the tool with the administrator account. Although this method works, I find it particularly annoying that the *Run as* dialog box used to enter the administrative credentials never remembers my AD account—I need to enter it for every situation in which I need to elevate my privileges.

My favorite solution to this challenge is to set up a centrally hosted terminal server where all relevant administration tools are installed. AD administrators can then connect to this terminal server, authenticate with their administrator account, and perform all required administrative tasks through the terminal server session. There's no requirement to use *Run as,* and I can even use RDP files on my desktop that are preconfigured with the correct account name. Of course you shouldn't opt to store the administrator's account password when saving the RDP files. Administrators can also use a central terminal server to connect from any client to perform their duties—the Windows Server Administration Tools Pack (adminpak.msi) tools don't have to be installed locally on the client. Many environments, however, might be too small to allow

IT Pro Hero

although the logon error had said the service was unavailable. Now Frank was really confused. Looking further at the query results, Frank noticed the State parameter. A State value of 4 means the service is running.

Homing in on the Problem

He ran the query command again without specifying a service and looked at the states of all running services. Eventually he noticed that the Netlogon service was paused. Perhaps this was the one thing keeping him out of the server.

He didn't have access to services.msc to start or stop the Netlogon service, but he had the SC tool. So Frank entered the following command to stop the Netlogon service:

```
sc \\192.168.10.10 stop netlogon
```

Then he queried to see the results of the previous command by entering

```
sc \\192.168.10.10 query netlogon
```

which showed him that the State value for Netlogon was now 2, meaning the service wasn't running. He then ran the following command to start Netlogon:

```
sc \\192.168.10.10 start netlogon
```

To see this command's results, he again queried Netlogon and saw that the service was running. Eureka! He had restarted the service from across the network by using the SC command-prompt tool.

Frank was now able to log on to the DC; all the GC server services were running and email was working. He had escaped from Command-Prompt Island and was back aboard the good ship GUI. It just goes to show you: Having the right tool is like wearing a life jacket when sailing in calm seas—you might not need it, but you'll be prepared should a sudden, unexpected squall hit.

InstantDoc ID 97507

Curt Spanburgh
(cspanburgh@scg.net) is a Microsoft Dynamics CRM MVP and a consultant for Solutions Consulting Group. He has worked with Microsoft applications for more than 20 years, and moderates the Microsoft Dynamics Support forum at www.minasi.com.

implementation of a terminal server purely for administrative purposes, or other reasons might exist for running the AD management tools from your local machine.

Another option to avoid the tedious and error-prone task of right-clicking the icons and entering your credentials is to create your own shortcuts that execute the Runas utility directly, fully leveraging its command-line options as well as those of the snap-ins themselves. And if your administrator accounts have a clear prefix or postfix added to the normal user account, you can leverage simple things such as the expansion of the USERNAME environment variables to further simplify managing shortcuts for multiple users.

As an example, my normal (unprivileged) user account might be called GUIDOG, whereas my administrative account is ADM.GUIDOG. To allow multiple administrators to use the same shortcut on different machines, I need to expand various environment variables in the shortcut I create, which is achieved by enclosing the respective environment variables between two percent signs. The following is a sample command for a shortcut I'd use to start the Active Directory Users and Computers snap-in with the administrative account and request that it binds to a specific DC in my domain:

```
%windir%\system32\runas /env /
  user:%userdomain%\adm.%username%
  "mmc %windir%\system32\dsa.msc /
  server=w2k8core01"
```

When I create the shortcut for this command, I can further enhance the warning effect and notify myself that I'm switching to a higher privileged account by using the color options of the shortcut itself—as for any command prompt, you can also configure background and font colors for a shortcut. Figure 2 shows the window that appears if I double-click the user GUIDOG shortcut. The command prompt's red background color warns me that I'm about to elevate my privileges. Because the *Run as* command in the shortcut appropriately expands %userdomain%\ADM.%username%, I no longer have to enter my account name. Instead I'm prompted to enter my password for the CORP\ADM.GUIDOG account right away.

Because Windows shortcuts are real files (with .lnk extensions), you can copy them to an appropriate share that's available to any other administrator in your AD forest. So if a different user, JOER for example, also has an administrative account using the same naming convention, he can use the same shortcut for launching the Active Directory Users and Computers snap-in and will be asked to authenticate as CORP\ADM.JOER.

Table 1: Caching Limitations of AD database with Different Windows OS Versions

Domain Controller Operating System	Standard LSASS Cache (max)	With 3GB Boot.ini Switch
Windows 2000 (32-bit)	0.5GB	1GB (3GB switch available only in Advanced Server edition)
Windows 2003 (32-bit)	1.5GB	2.6GB
Windows 2003 x64	8TB	N/A

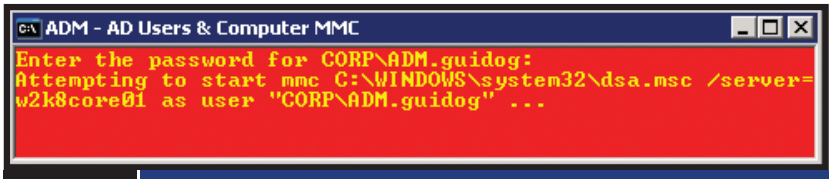


Figure 2: Starting the Active Directory Users and Computers snap-in with a specific DC as a privileged user

64-Bit Windows Challenges

The current trend is a strong move toward 64-bit Windows versions, especially for applications that can benefit from the increased memory space that 64-bit OSs offer. AD is one of those applications—if your AD database doesn't fit within the memory limitations that it incurs on 32-bit Windows Server versions (which Table 1 shows), upgrading your DCs to 64-bit Windows on hardware with sufficient physical memory can greatly improve AD's performance, as well as the performance of dependent applications (e.g., Exchange).

I won't go into the details of when and where you should consider leveraging 64-bit Windows for your DCs. In general, you won't run into any problems combining 32-bit DCs with 64-bit DCs in your AD forest (e.g., leveraging Windows Server 2003 x64). No 64-bit–specific schema extensions are required, and 64-bit DCs replicate just fine with their 32-bit counterparts. Of course you need to ensure that you have proper versions of your drivers, antivirus software, and monitoring agents that support your 64-bit Windows OS. However, some of the Microsoft AD-related management tools that used to run on your DCs might no longer function. The most important ones that I know of are the AD Replication Monitor support tool (Replmon), the Group Policy Management Console (GPMC), and the Active Directory Migration Tool (ADMT) Password Export Server (PES) service. Most 32-bit applications run with no problem on a 64-bit Windows OS because they leverage the OS's Windows-on-Windows 64-bit (WoW64) compatibility feature. Replmon, GPMC, and ADMT PES are true exceptions to this rule because they have other dependencies that WoW64 can't meet. Replmon and GPMC run without a problem on a 32-bit member server and can thus be further leveraged in a pure 64-bit AD forest and connect remotely to the 64-bit DCs. ADMT PES must be installed on a DC, so you either need to have a 32-bit DC that you can leverage for this service, or you need to wait for the upcoming ADMT release—which is slated for release with Windows Server 2008 and will include a 64-bit version of the PES service.

Forewarned Is Forearmed

AD is a powerful directory and authentication service. Its multi-master replication model ensures the high availability that companies request from such an important service. But sometimes the small things that might not work as expected are the ones that cause the most pain for an administrator. Knowing about some of these annoyances ahead of time will hopefully help you avoid them in your own infrastructure.

InstantDoc ID 97611

Guido Grillenmeier

(guido.grillenmeier@hp.com) is a master technologist with Hewlett Packard's Advanced Technology Group. He is a Microsoft Directory Services MVP and a Microsoft Certified Architect. He is the coauthor of *Microsoft Windows Security Fundamentals* (Digital Press).

Introducing:

Sunbelt Exchange Archiver™

Finally, Affordable Enterprise-Class Archiving

Introducing Sunbelt Exchange Archiver. Sunbelt Exchange Archiver (SEA) is a robust new product which delivers real enterprise-class email archiving, at a price that won't break your budget. Get comprehensive legal and regulatory compliance. Reduce your Exchange storage by up to 80%. Securely store emails on your choice of media, using the built-in Hierarchical Storage Management. And, find archived emails rapidly with full-text search for e-discovery or compliance.

Compliance, e-Discovery, and legal readiness. If you need to archive emails for regulatory or legal reasons, SEA has you fully covered. Emails are stored in their original form, in whatever secure media you prefer, with complete flexibility on retention. Need to find an archived email? Simply use SEA's powerful integrated full-text search of emails and attachments, and you'll be ready at a moment's notice for e-discovery or legal requests.

Seamless end-user experience. SEA is fully transparent for your users, whether they're running Outlook, OWA, Blackberry devices or even Entourage on the Mac – with no special client software needed. Trusted end users can be delegated granular authority with the included web-interface or optional Outlook add-in. They can do off-line synchronization, and search, edit, forward, move or delete archived emails.

"Exchange performance is suffering. Your users complain about email storage. Your CEO wants legal compliance. Now what?"

Up to 80% smaller message store. With SEA, you'll dramatically reduce your Exchange storage. The benefits are clear: faster backup times, better Exchange performance, and faster recovery.

Journaling not required. It's a fact that using the Exchange Journaling mailbox for archiving dramatically affects server performance. With SEA, Journaling is an option – the program's breakthrough Direct Archiving feature stores all emails immediately after they are received, keeping load off the Exchange server.

No more PST headaches! SEA gets rid of pesky PST files that are a major admin headache. SEA automatically finds them, imports them, and makes them part of your user's archive.

Great for disaster recovery. No matter where you email is stored, business continuity is assured with SEA. Using the included web client, users can continue to see and use their email even if Exchange is down.

Archiving's time has come for everyone. Contact us today and see how SEA solves your legal and compliance headaches and immediately improves the performance of Exchange – while saving critical budget dollars.

Sunbelt Software

Get A Free Quote and See How SEA Compares to Symantec Enterprise Vault™!

Email sales@sunbeltsoftware.com or call 888-688-8457

Sunbelt Software Tel: 1-888-688-8457 or 1-727-562-0101 Fax: 1-727-562-5199 www.sunbeltsoftware.com sales@sunbeltsoftware.com

PROBLEMS WITH PERMISSIONS

Windows file server annoyances

BY DAN HOLME
ILLUSTRATION BY RYAN ETTER

The Server service has been part of Windows NT–based OSs since day one, and the vast majority of Windows servers are file servers. You'd think that we IT professionals and Microsoft would have this file-server thing ironed out by now. Unfortunately, that's not the case. I've heard from countless business clients (and these aren't mom-and-pop shops) that IT still isn't configuring file servers right. And Microsoft isn't helping. In fact, in some cases Microsoft is adding to the problems in its newest OS versions by creating what I call "tools for dummies," such as the new Windows Server 2008 Share command, which isn't customizable and applies really poor default configurations. Although file servers are one of the most common causes of annoyance for IT, the situation isn't hopeless. You can align file server technologies with business requirements, and I'll show how you can work around the problems with permissions, such as Full Control or Modify, and some of their defaults, such as the default inheritance of the delete permission, that Microsoft wants you to use.

Full Control or Modify

Most of us know the dangers of Full Control. Fewer of us have considered scenarios in which Modify is a risky permission to apply. I can write pages on the dangers of assigning Modify and Full Control permissions to groups, but I'll narrow down my scope here to one of the most severe problems these permissions can cause: granting Delete permission.

In most collaborative file-sharing scenarios, such as sharing a team folder, a group of information workers receives Modify or Full Control permission. The danger is that Modify and Full Control permissions templates include the Delete permission, which applies by default to "this folder, subfolders, and files." With this permission and its inheritance, a user in the group can delete any and all files and subfolders. In other words, anyone on the team can select a folder and press the Delete key. Say *au revoir* to your data and hello to denial of service. Such a deletion could be malicious or accidental, but it can be prevented.

Spend some time defining the requirements of your collaborative shared folders, and be aware that permissions used for good can also be used for evil. You'll find that, depending on the requirements of the particular folder you're granting permissions for, you can solve the Delete problem in a number of ways. First, you can give the whole group Allow::Write permission, which lets anyone in the group create and change files and folders. Then, give a more restricted group the Delete permission. Second, you can grant the group Modify permission but change the scope of the permission to apply to Files only. This still allows an accidental or intentional deletion of files within the folder, but it stops the recursive deletion of subfolders in the event of an accidental deletion.

Delete Subfolders and Files

Even more perilous is the Delete Subfolders and Files permission, an access control entry (ACE) in the Full Controls permission template. A user with this permission on a folder can delete any subfolder or file within the folder, even if the user has explicit Deny:: Delete permission. So, any user who's a member of a group with Full Control of a folder can delete all of its contents, creating a denial of service situation. This is far worse than the standard Delete permission because Delete Subfolders and Files overrides all other permissions, including explicit Deny permissions. It's a doozy in the wrong hands.

To avoid this problem use Best Practice Number Two: Be extremely careful about granting Full Control. I recommend restricting Full Control to System. Give the Modify permissions template plus Change Permissions permission to support groups who need to change folder permissions.

By the way, Best Practice Number One is: Always assign permissions to groups, not users. This point leads me to the next annoyance.

Creator Owner ACE

Most organizations have increased their focus on security policy, which makes defining rules for access essential. For shared folders, the parent folder ACL determines the access policy. A team shared folder, for example, is typically set to allow team members to read each other's files. Often they can add files to the share, and sometimes they can even change each other's files. The problem is that on each new folder, there's a default ACE that gives the *Allow::Full Control (Apply To Subfolders and Files)* permission to the special identity Creator Owner. When a user creates a file or folder, the ACE assigned to Creator Owner is applied to that specific user.

So, for example, if Dan Holme joins the team and creates a new file in the team share, he receives Allow::Full Control permissions for that file. What if Dan leaves the team? He's removed from the group that can read and create files in the share. But he can still access his file because he has an explicit Allow::Full Control ACE on that file. So just because Dan created the file, he's exempt from the entire shared folder's access policy, which specifies that only team members have access. Even if an administrator uses the Change Owner function to assign the file to another team member, Amy, Dan still has his explicit permission (and Amy does *not* inherit Dan's Full Control permission) unless the administrator changes the file's permissions.

To fix this annoyance, analyze the capabilities needed by the shared folder users. You might decide to remove the Creator Owner ACE. If you've assigned team members the Allow::Write permissions template so they can change each other's files on the share, you don't need the Creator Owner ACE. Without this ACE, when Dan joins the team and creates a file, the new file inherits the access policy of the parent folder but doesn't add an explicit ACE for Dan. He can modify his file because he's on the team, but when he leaves the team, his access is removed. There's one more catch: Dan can, as owner, return to the object and give himself permissions. We'll solve that one next.

Changing Permissions

Every organization has battled problems caused by users maliciously or inadvertently changing permissions on files or folders they've created. Windows provides an implicit permission (WRITE_DAC) to the security identifier (SID) of the user who owns a file or folder. WRITE_DAC enables the user to change permissions on the object, even if he or she wouldn't otherwise have Allow::Change Permissions. This ability represents a significant security problem because the owner of a file or folder can change the access policy defined by the ACL on the parent folder.

Prior to Windows Vista, the only viable solution was to change the Server Message Block (SMB) permissions (i.e., share permissions). Most administrators use Allow::Full Control as the SMB permission. But if you change it to Allow::Change, the more restrictive SMB permission will allow every action *except* changing permissions.

Vista and Windows Server 2008 make it even easier to solve the problem by adding a new special identity, OWNER RIGHTS, which represents the current owner of a file or folder. Permissions assigned to this identity will set the permissions for the owner, overriding the owner's implicit rights, including the right to change permissions. So the new best practice is to assign OWNER RIGHTS::Allow::Modify. The Modify permission doesn't include the Change

Learning Path

WINDOWS IT PRO RESOURCES

"File and Print Annoyances," InstantDoc ID 94675

"Modifying Folder and File Permissions," InstantDoc ID 50461

MICROSOFT RESOURCES

Windows Administration Resource Kit: Productivity Solutions for IT Professionals,

microsoft.com/MSPress/books/11297.aspx

"How to set, view, change, or remove special permissions for files and folders in Windows XP,"

support.microsoft.com/kb/308419

Permissions, Delete Subfolders and Files, and Take Ownership permissions included in the Full Control permissions template. As soon as your file servers are running Server 2008, this annoyance will be history.

Users See but Can't Access

When users open folders, they can see all of the contents, by default, including files and folders to which they don't have access. I don't have a problem with such visibility: As long as the file or folder can't be opened, visibility doesn't really matter. However, if it matters to you, here is my guidance: Reorganize your files and folders or implement Access-Based Enumeration, which is available for Windows Server 2003 from Microsoft's downloads site at microsoft.com/downloads/details.aspx?FamilyID=04A563D9-78D9-4342-A485-B030AC442084&displaylang=en. (For more details, see the *Windows IT Pro* "File and Print Annoyances" article, February 2007, InstantDoc ID 94675.)

Shared Folder Delegation

There's a Windows 2000 and Server 2003 annoyance—setting permissions for shared folders—that makes me want to read the riot act to the product team at Microsoft. This annoyance is so big and multifaceted that I can't begin to do it justice here. (So if anyone at Microsoft is listening, call me!) At the core of the problem is the delegation of permissions to create shared folders.

Let's assume you're in an organization with more than one level of administrator. The organization has technical support people responsible for the servers. These folks work on hardware, backup, configuration, patching, and so forth—the tasks of real Administrators with a capital "A." In Windows, a member of the Administrators group can do anything and get to anything on a server. Let's say there's also a support role with the task of creating a shared folder. To me and to every client I work with, this task is at a lower escalation level than the other tasks Administrators perform. Unfortunately, to Microsoft, these two types of tasks are equal. To create a share, you must be a member of a privileged group such as Administrators, Power Users, or Server Operators, and these groups have additional hard wired rights as well. Microsoft doesn't provide a way to delegate the ability to create a shared folder to someone lower in the administrative hierarchy.

I was excited when I learned that Windows XP's PowerToy, Tweak UI, exposed a way to delegate this ability. But, unfortunately, TweakUI isn't an official part of Windows and Microsoft doesn't support it. The permission to create a share is a binary registry entry, and changing it's also not supported. So, I'm sad to say, the only way to delegate creation of shared folders is to put technical support groups into the local Server Operators or Power Users group on a member server. At least you can avoid giving them Administrators credentials.

But the fun doesn't end there. When you create a shared folder, you want to configure its settings: permissions, caching, access-based-enumeration and perhaps its description or connection limit. The settings for the first three are the most useful and common. How do you configure them other than using the shared folder user interfaces? How can you use a command line or script? Permissions can be set from the UI or a command line (i.e., by specifying NET SHARE), but not through a VBScript. Caching settings can be set from the UI or the NET SHARE command, but not through a VBScript. Access-Based Enumeration can be enabled only in the UI. There's no command line, and the NetShareSetInfo function isn't something mere mortals can script. How's that for consistency? It sure makes automating the creation of shares difficult for non-developers.

Finally, the default settings for a new shared folder are lousy for the vast majority of shared folders. Everyone::Allow::Read is the default share permission that restricts everyone, even administrators, from any higher-level access, even if NTFS permissions define more permissive access policies. Every client I've worked with recently has very clear policies indicating that Full Control is the correct share permission in almost every scenario and that NTFS permissions define actual access policy. This is an example of Microsoft locking down something too far and not giving customers a way to change the default to something useable.

Similarly, the default caching settings enable users to "pin" any file in the share to make it available for offline access. With any multi-user folder other than a read-only folder, this ability opens up possibilities for offline editing and conflicts on synchronization. Because of the security implications I recommend that you consider locking down the default access for offline files.

To change the default caching settings use a script or the command line to provision and automate your shares. The NET SHARE command, for example, provides an easy way to create a shared folder, including switches for configuring the Full Control share permission and for disabling offline files for the share:

```
/GRANT:Everyone,Full
```

and

```
/CACHING:None
```

File Sharing for Dummies

Everything I just discussed applies in Vista and Server 2008. Alas, Server 2008 continues down the wrong path. So consider this section a preview of Server 2008 annoyances.

My first Server 2008 annoyance is the Share command: Don't even think of choosing the Share command on the context menu in Windows Explorer. The new Share command is reduced to "File Sharing for Dummies." It displays the File Sharing dialog box shown in Figure 1, page 38.

In the File Sharing dialog box, you can change the Permission Level to Reader, Contributor, or Co-Owner. This dialog box sets both the share and the NTFS permissions to Read, Change/Modify, or Full Control. That implementation of permissions goes against the written policy and procedure of just about every client I've ever had. Typically policies require that shared folder permissions be Full Control and that NTFS permissions define access policy. And, because most of us learned to secure a folder before sharing it, we may have actually spent some time creating the perfect ACL. But this command won't share the folder for any group that has anything other than standard Read, Modify, or Full Control NTFS permissions templates. Try securing a folder so that a team has Write permission and then try sharing it. You'll see that the group isn't given any share permission.

This annoyance gets worse because of the way Microsoft implements the roles in the dialog box. In most role-based security models, including Microsoft's own SharePoint and Exchange public folder models, a Contributor doesn't Modify, an Editor does. The difference between the Contributor and Editor roles is that a Contributor can add something and

can change his or her contribution. In contrast, an Editor can change a file from any contributor. Now whether you agree with those definitions of Editor and Contributor or not, the real point is that Microsoft is making assumptions about the understanding every client has regarding roles. It doesn't provide any options for a company to change what the dialog box does.

Finally, Microsoft rubs salt in the wound by putting this tool that I call "File Sharing for Dummies" in the same place the tried-and-true (and effective) Share interface used to be. You now have to look for the Advanced Sharing command to get to the settings you really need. And here's my question: Because you have to be in a privileged group (such as Administrators) to share a folder and because we're dealing with a server OS, can't we assume that Administrators know what they're doing? Even the very nice Provision a Shared Folder Wizard in Server Manager has crazy defaults—such as Everyone::Allow::Read and Caching=Manual—that you can't customize for the needs of your organization.

The best solution for these Server 2008 annoyances is using the Net Share command or other scripts to provision shared folders with exactly the settings you require. Even the brilliant new PowerShell has no way to set all the Server Message Block (SMB) settings of a shared folder. Annoying.

Figure 1: Changing permission levels in the File Sharing dialog box

Final Annoyance

The list of file server annoyances and solutions is far too long to detail in just one article. So watch this space for future articles. For further resources, see the Learning Path on page 36.

InstantDoc ID 97619

Dan Holme
(danh@intelliem.com) is director of consulting at Intelliem, which delivers solutions-focused training and consulting services supporting enterprise SharePoint, Office, Windows, and Active Directory implementations.

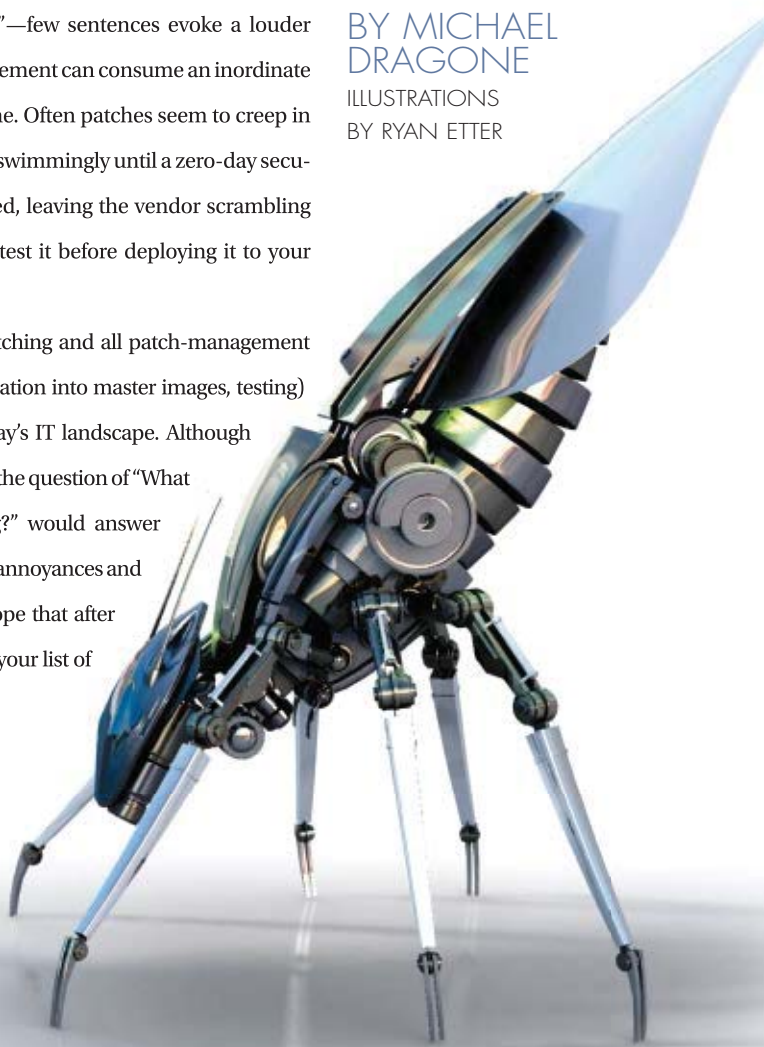
MANAGE THOSE PESKY PATCHES

BY MICHAEL DRAGONE
ILLUSTRATIONS BY RYAN ETTER

"You have to download a patch"—few sentences evoke a louder groan from IT pros. Patch management can consume an inordinate amount of your already limited time. Often patches seem to creep in from nowhere—everything is going swimmingly until a zero-day security flaw is discovered and publicized, leaving the vendor scrambling to provide a patch and you scrambling to test it before deploying it to your production systems.

The fact is that patching and all patch-management tasks (downloading, integration into master images, testing) are a necessary evil in today's IT landscape. Although most of you if presented with the question of "What about patch management do you find annoying?" would answer "Everything!", I've dealt with some specific patching annoyances and figured out how to make them less annoying. I hope that after reading my tips you'll be able to cross patching off your list of IT annoyances.

YOU'LL NEVER DREAD PATCH TUESDAY AGAIN



Prior Patch Preparation

The first patching annoyance that I'll cover is the simple problem of finding out what patches are available and what issues they address. IT pros the world over are intimately familiar with Microsoft's usual patch release day—the second Tuesday of every month, better known as Patch Tuesday. But there's no reason to blindly check Windows Update on Patch Tuesday and install everything offered on a test machine and hope for the best.

At the Microsoft Web page "Microsoft Technical Security Notifications" (www.microsoft.com/technet/security/bulletin/notify.mspx) you can sign up for the Comprehensive Alerts email notification or the RSS feed (or more likely, you'll want to sign up for all of the alert services on that page). Doing so provides you with early notification about the number of updates and the severity rating of security updates that Microsoft is planning to release on each Patch Tuesday. These bulletins are released the Thursday before Patch Tuesday.

On Patch Tuesday, you'll receive another notification that provides further details on the released patches, including how to get more information. Sometimes Microsoft will release an out-of-band update to address an exceptionally dangerous security vulnerability. Notifications of these updates are also included in the alert services offered on the page noted above.

Also be aware of what I like to refer to as Stealth Patch Tuesday. Microsoft sometimes releases non-security updates on Tuesdays other than the second Tuesday of the month. This is why you'll be working on your computer on, say, the fourth Tuesday of the month and see the "Updates are available" balloon notification pop up.

You should also keep the Microsoft Security Response Center (MSRC) blog (blogs.technet.com/msrc/default.aspx) in your arsenal of Microsoft patch planning. Here, members of the MSRC not only reiterate the information provided by the notification service mentioned above, they also offer additional insight into the security patch release process and address problems that occur after Microsoft releases a patch. If there's a buzz around a particular Microsoft security patch, be it a stability, deployment, or compatibility issue, you can be sure the MSRC team will address it.

Now that you're prepared for when Patch Tuesday arrives, how do you know if a security vulnerability is already being exploited in the wild? A quick way to check is to examine the last two FAQ answers under the security bulletin in question.

Let's take bulletin MS07-051 as an example. The bulletin is located at www.microsoft.com/technet/security/bulletin/ms07-051.mspx and the section we're interested in is under the Vulnerability Information heading. Expand the section containing the CVE number (in this case it's "Agent Remote Code Execution Vulnerability - CVE-2007-3040"), then expand the last section containing the FAQs. You're interested in the answers to the last two questions. Skipping to the FAQ section about possible exploits doesn't mean that you shouldn't understand and plan to deploy all relevant patches to bring your systems up-to-date; it simply lets you quickly prioritize your patching schedule to first address those issues which can be exploited and cause you the most pain.

Even though I'm focusing on Microsoft, it's rare to be in a homogeneous IT environment these days. So what about security patches for products not developed by Microsoft? For these you can either look on the vendor's Web site for a similar security or patch notification service or invest some time daily at Secunia (secunia.com) and SecurityFocus (www.securityfocus.com). Better yet, subscribe to their respective RSS feeds that are relevant to the systems you support.

THERE'S NO REASON to blindly check Windows Update on Patch Tuesday and install everything offered on a test machine and hope for the best.

Your New Best Friend: WindowsUpdate.log

Patch Tuesday has come and gone. You've tested a patch and are ready to deploy it into production. In many IT environments these days, you'll do this using Windows Server Update Services (WSUS). Smaller shops and home office users will likely have the Automatic Updates service turned on.

However, sometimes it might appear that WSUS and Windows Update (including the superset, Microsoft Update) aren't cooperating with one or more computers. You might find that Windows Update also isn't much help in providing a solution, offering only a generic error message and a cryptic hexadecimal code. So what should you do?

Take a look at WindowsUpdate.log, located in your Windows installation directory (typically C:\WINDOWS). One way to do so is to go to Start, Run and type

```
%windir%\windowsupdate.log
```

You'll want to search the file for the words FATAL and WARNING, paying careful attention to the lines that immediately precede the FATAL or WARNING message. You'll also want to note any error codes provided and search on those codes in your favorite Internet search engine and in the Microsoft Support Knowledge Base. (For more information about WindowsUpdate.log, see the Microsoft article, "How to read the Windowsupdate.log file" at support.microsoft.com/kb/902093.)

One major annoyance I ran into recently occurred with a new, out-of-the-box machine running Windows Vista Business. The machine correctly received the Group Policy Object (GPO) containing its update settings, including the correct WSUS server. However, the machine refused to download any updates. Searching the WindowsUpdate.log file, then searching the Microsoft Support Knowledge Base for the error code, I found the solution—stop the Automatic Updates service, empty the SoftwareDistribution directory under the Windows installation directory, then restart the Automatic Updates service.

Your potential. Our passion.®

Microsoft®

beating the mummy. easy.

1. Know your hieroglyphs.
The ancient hieroglyphs speak of the pharaoh's return, and his vicious attack on a midsize enterprise IT department. How it all turns out is less clear, as the hieroglyphs got chipped and are hard to read. Sorry.

2. Make a torch.
The Mummy, being wrapped in dry linen, is extremely flammable. Make a torch from a rolled-up newspaper and swing it in his direction. You'll get his attention immediately and he'll quickly lurch away.

3. Unwind him.
The Mummy is easy to unwind. Sit him in a swivel chair, grab his loose end, and spin. Keep him spinning, make him dizzy, and once you're done, he'll be completely exposed.

4. Summon the sun god Ra.
Borrow an ancient staff or a magic ankh. Speak the magic words to summon the mighty power of the sun god Ra, and stand back, because Ra does not mess around once summoned.

5. Be the Mummy's daddy.
Ancient Egyptian royalty was dynastic, meaning the pharaoh's firstborn child became the pharaoh. Disguise yourself as an older Mummy, tell the Mummy you're his grandfather, and he'll be obligated to do your bidding.

beating hackers. easier.

1. Implement Microsoft® Forefront.™
Forefront makes defending your systems easier. It's a simple-to-use, integrated family of client, server, and edge security products (such as IAG 2007) that helps you stay ahead of your security threats more easily than ever.

For case studies, free trials, demos, and all the latest moves, visit **easyeasier.com**

Microsoft®
Forefront™

SOMETIMES A TRANSIENT ERROR ISN'T TRANSIENT AT ALL. When a patch is annoying you, save yourself a heap of time by taking five minutes to research it before you wildly try to fix the problem.

When a Patch Is Too Big

The problem of a patch being too big drove me up a wall. I had purchased an HP server and was eager to get it up and running to test Microsoft Forefront Client Security. The server hardware was running flawlessly, as was Windows. I had no trouble installing many of the base components required for Forefront Client Security, including WSUS 3.0 and Microsoft SQL Server 2005. Before I installed Forefront Client Security itself, I decided to take one more trip to Microsoft Update to ensure that none of the products I had just installed required any updating.

As it turned out, part of the SQL Server 2005 installation included some Microsoft Visual Studio 2005 components. Visual Studio 2005 SP 1 was available, so I fired off the download and installation. The installation failed. I didn't bother to note the error code, figuring it was a transient error. It was the end of the day so I decided to shut the server down and try again the next morning.

The definition of insanity is performing the same task repeatedly and expecting different results, yet insanely I repeated the same steps the next morning, in hopes of a different outcome. I got the same results, of course. Thinking it might be a problem with Microsoft Update, I downloaded VS SP1 directly from the Microsoft Download Center, bypassing Microsoft Update entirely.

As you might have guessed, installing VS SP1 by this method produced the same result. Having installed VS SP1 several times previously on machines that were far less "clean" than this one, I was perplexed. I did, however, wisely note the error code I had been repeatedly given: *Error 1718. File [.msp filename of SP1] was rejected by digital signature policy*.

The error code was even more perplexing as I was certain this machine had no policy on it that would prevent this installation. Furthermore, I couldn't imagine that this file wasn't correctly signed by Microsoft. Off to the Microsoft Knowledge Base I went, where I found the Microsoft article (support.microsoft.com/kb/925336/en-us) detailing my exact problem and offering a link to the hotfix that corrects it. In short, Windows Installer attempts to load the entire .msp package to verify the digital signature but can't allocate enough contiguous memory and fails with the error above.

Sometimes a transient error isn't transient at all. When a patch is annoying you, save yourself a heap of time by taking five minutes to research it before you wildly try to fix the problem.

Update Déjà Vu

I've seen another problem occur numerous times, and it's still as annoying as it was the first time I encountered it. Here's what happens: You download updates via Windows Update. You restart with a heavy sigh, then return to Windows Update only to find the exact same update offered to you again. Thinking the update didn't install properly, you install it again and restart. Windows Update continues to offer you the same update. What gives?

In some cases, the update truly isn't installed. Verify that the update is indeed installed by looking in your update history at the Windows Update site. The update status column should read "successful."

In other cases, the detection logic that Microsoft provided for this particular update has a problem that is causing Windows Update to think that you haven't installed the update when you already have. Although you can't fix this yourself—Microsoft has to correct the detection logic—the update was successfully installed and is working, but Windows Update doesn't realize it. The MSRC blog is a good first stop if you think you're having this problem, as members of the MSRC team will almost always drop a note indicating that the detection logic needs to be changed.

Computers Missing in Action

The problem of computers missing in action is only slightly less annoying than the repetition of updates. You're missing one or more computers in your WSUS console. You know the settings have been correctly deployed with Group Policy as some computers are showing up, but some never appear no matter what you try.

Computers can go missing if a Windows installation wasn't prepared for image duplication by using Sysprep. Subsequent images therefore have a duplicate SusClientID in the registry. It's unlikely that you'll run into this problem on a regular basis and the fix for it is relatively easy. First, stop the Automatic Updates service on the computer experiencing the problem. Then, start the registry editor and navigate to the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate subkey and delete the PingID, AccountDomainSid and SusClientId entries. Restart the Automatic Updates service, then run the following from a command prompt:

```
wuauclt.exe /resetauthorization /detectnow
```

You can also use the /detectnow switch (without /resetauthorization) if you've recently approved updates on your WSUS server and want to force a machine to run a detection cycle prior to the next scheduled cycle.

The Long Haul

No piece of software is perfect. Despite the annoyances they cause, patches are here to stay. The trick to managing them is to be informed, stay vigilant, and get up-to-date!

InstantDoc ID 97551

Michael Dragone
(mike@mikerochip.com) is a Systems Engineer for a title insurance company in New York. He is a MCDST and a MCSE: Messaging and remembers when *Windows IT Pro* was called *Windows NT Magazine*.

Microsoft Exchange Server 2007 SP1: AN OVERVIEW

BY KIERAN MCCORRY

With improvements to unified messaging and support under Windows Server 2008, this service pack has much to offer Exchange administrators

Microsoft Exchange Server 2007 SP1 introduces a wealth of new functionality that will interest messaging system architects and administrators. Microsoft has previously differentiated between service pack releases, intended to address bugs and other minor flaws, and feature pack releases, which add significant new functionality to the base product. That definition certainly indicates that Exchange 2007 SP1 is as much a feature pack release as a service pack. Let's take a look at the enhancements coming in SP1 and see what they might mean for your organization.

Standby Continuous Replication

Chief among the new features in SP1 is standby continuous replication (SCR). Microsoft introduced local continuous replication (LCR) and cluster continuous replication (CCR) with Exchange 2007. LCR, as its name suggests, replicates database transactions to another local disk on the same Exchange 2007 server. LCR is useful if you lose a database or the drive that hosts a database because another copy is available that's been kept up to date by using LCR's log shipping and replay technology, but LCR is limited because it replicates data only within the same Exchange server. In contrast, CCR provides replication of database transaction data between two nodes in a cluster. This technology is focused on high-availability and failover scenarios and obviously requires the use of Exchange clusters.

Enter SCR. This solution arguably falls somewhere between the functionality of LCR and CCR. LCR focuses more on the notion of data copying than data protection and high availability. With SCR, you can replicate database log files to another Exchange 2007 server anywhere in your Exchange organization, provided it's in the same Active Directory (AD) domain, though it need not be in the same AD site. Therefore, SCR lets you replicate mailbox databases to locations that might be geographically remote from your source Exchange server.

SCR gives you more flexibility than LCR because the replication is off-node and more flexibility than CCR because you aren't limited to a single Exchange cluster to host the source and target nodes of the replication. If you lose the source server with SCR, you still have a copy of the data elsewhere on your network; you can either rebuild the server and copy the data back or use the replicated mailbox

data on another server and rehome affected users. You can also combine SCR with LCR or CCR technologies. A source server can have LCR enabled as well as SCR to a remote location; similarly, a source server can be a cluster member either with or without CCR enabled.

Unlike LCR and CCR, SCR lets you replicate data for a given storage group to multiple locations. So, for that really important database, you can have replicated copies of the transaction logs in several locations. Similarly, an SCR target can have multiple sources—you can designate a single Exchange server in a remote location to be the SCR target for many different source servers. Just like LCR and CCR, you can use SCR only on storage groups that contain a single database, but you can have multiple storage groups replicated using SCR. SCR requires that both the source and target servers are running SP1 and also that an SCR target can't be running LCR. SCR doesn't provide any automated way of failing over databases if a problem occurs on the source server. You'll have to construct the operational procedures appropriate to how you deploy SCR within your organization.

Learning Path

WINDOWS IT PRO RESOURCES

To learn more about Exchange 2007 SP1:

"What to Expect from Exchange 2007 SP1," InstantDoc ID 95478

"Exchange 2007 SP1: The Inside Scoop," InstantDoc ID 96892

"SCR in the Spotlight," InstantDoc ID 96372

"Standby Continuous Replication in Exchange 2007 SP1," InstantDoc ID 96888

"S/MIME and Exchange 2007 SP1," InstantDoc ID 96998

To learn more about deploying Exchange 2007:

"Designing Your Exchange Server 2007 Infrastructure," InstantDoc ID 95687

"Upgrading to Exchange Server 2007," InstantDoc ID 96241

"Upgrading to Exchange Server 2007, Part 2," InstantDoc ID 97357

"Configuring Exchange Server 2007," InstantDoc ID 96044

"Designing Active Directory for Exchange Server 2007," InstantDoc ID 96536

"A Trip to the Store with Exchange 2007," InstantDoc ID 96731

"Configure POP and IMAP in Exchange 2007," InstantDoc ID 95840

MICROSOFT RESOURCES

"What's New in Exchange Server 2007 SP1"
technet.microsoft.com/en-us/library/bb676323.aspx

"Standby Continuous Replication"
technet.microsoft.com/en-us/library/bb676502.aspx

"Cluster Continuous Replication"
technet.microsoft.com/en-us/library/bb124521.aspx

"Local Continuous Replication"
technet.microsoft.com/en-us/library/bb125195.aspx

"Flush and reset a client resolver cache using the ipconfig command"
technet2.microsoft.com/WindowsServer/en/library/a184e334-2c9f-48c4-abe7-804188200dd91033.mspx?mfr=true

"New High Availability Features in Exchange 2007 SP1"
technet.microsoft.com/en-us/library/bb676571.aspx

"New Transport Features in Exchange 2007 SP1"
technet.microsoft.com/en-us/library/bb684905.aspx

CCR Improvements

In Exchange 2007 RTM, all transaction log copying for CCR takes place over the public network in the cluster, which can cause communication problems. For example, when the passive node comes back online after being unavailable, you can get bottlenecking due to CCR replication contending with normal client traffic. Also, if the public network fails, a failover can take place without all transaction log data being replicated, despite the data being available.

With SP1, administrators can create mixed networks to take care of log shipping. For example, you can use the internal cluster network (which usually carries just the cluster heartbeat traffic) to ship logs between servers and so avoid contention with client traffic. SP1 also brings general performance improvements for clusters, including reduction in I/O for CCR and improved clustered Mailbox server transition when using CCR.

Exchange 2007 Meets Windows Server 2008

Although Exchange 2007 RTM isn't supported on Windows Server 2008 (previously codenamed Longhorn), SP1 is designed specifically to work with Server 2008. SP1 exploits Server 2008's improved clustering support, enhancing Exchange 2007's overall clustering capability.

Without SP1, Exchange 2007 clusters are supported only on Windows Server 2003 and can't span multiple IP subnets. Add SP1 and Server 2008, and the IP subnet limitation is removed—Exchange clusters can now be geographically dispersed across separate IP subnets. This capability simplifies the creation and management of infrastructures for wide-area Exchange clustering: virtual LAN technology between remote data centers, for example, is no longer required.

This new functionality brings with it new challenges. If a Mailbox server in a wide-area cluster fails over to a node in a different IP subnet, the IP address of the Mailbox server will change even though the DNS name of the server stays the same. SP1 uses routable protocols for clusters, as opposed to the broadcast-style protocols of pre-SP1 clusters. Therefore, clients must be able to connect to the remote failover node using DNS because the failover process dynamically updates the DNS entry for the clustered Mailbox host. For this reason, Microsoft recommends using a short Time to Live (TTL) value for clustered Mailbox DNS records. Administrators also need to pay attention to the local DNS cache on client computers; to ensure that DNS resolution takes place using valid data after a failover, you can run the Ipconfig command with the /flushdns switch on client computers. You might be able to implement this procedure with a logon script, or perhaps a desktop icon to execute the command would be appropriate.

Implementing SP1 on Server 2008 also provides messaging architects and administrators an opportunity to brush up on their IPv6 skills: IPv6 native networks are supported with Exchange 2007 SP1. However, this is a tricky area because DHCP IPv6 isn't supported on Server 2008; only static addresses are supported. SP1 includes several new setup options for /NewCMS and /RecoverCMS relating to clustered Mailbox server configurations in both IPv4 and IPv6 environments.

OWA Gets Back What It Lost—and More

Outlook Web Access (OWA) for Exchange 2007 was completely rewritten from the version for Exchange 2003. Unfortunately, not all of the OWA 2003 features were ported to OWA 2007, due largely to time constraints. Some of these previous OWA features are returned in SP1 and some new features have been added as well.

OWA Light has been enhanced with activity monitoring so that the session isn't timed out if, for example, it takes a long time to enter a message. Also, when messages are being composed, they're automatically saved in the

Drafts folder if the session times out because of inactivity. This is a welcome improvement for avid OWA Light users.

The experience for OWA Premium users is improved as well. Users can now create and edit Personal Distribution Lists, create and edit server-side rules, and access the Recover Deleted Items feature. Users will be happy to see that access to Public Folders from the OWA Premium client is back. OWA Premium's WebReady Document Viewing now supports Office 2007 so that these files can be viewed in HTML format. OWA Premium also adds a monthly calendar view (previously it had only daily and weekly views) and support for Secure MIME (S/MIME) for receiving and sending of signed or encrypted email.

Exchange Transport Improvements

SP1 has a range of different transport improvements that cut across core transport functionality as well as specific improvements for the Edge Transport and Hub Transport server roles. Core transport functionality has been improved specifically in the back pressure feature. This feature helps you monitor key resources such as free space on drives that hold message queue databases and transaction logs, the number of uncommitted message queue database transactions in memory, and memory utilization by EdgeTransport.exe and other system processes. With back pressure, if system resources become too heavily utilized, Exchange stops accepting new messages to prevent the server's resources from becoming completely exhausted. The net result is that the overall stability and reliability of the Exchange system is improved. The disk space requirements for back pressure have been refined from 4GB in Exchange 2007 RTM down to 500MB in SP1. SP1 also adds additional options for configuring other transport feature settings.

SP1 optimizes the basics of message processing for the Hub Transport role. Some of the specific enhancements include:

- priority queuing so that the categorizer takes into account user-set priorities on messages
- adding a MaxMessageSize parameter to the Set-AdSiteLink cmdlet so that an administrator can set a maximum message size for messages relayed between AD sites
- adding a MaxMessageSize parameter to the New-RoutingGroupConnector and Set-RoutingGroupConnector cmdlets for controlling maximum sizes of legacy Routing Group Connectors
- controlling the scope of Send connectors to AD sites
- enabling transport rules to act on unified messaging (UM) messages
- enhancements for Windows Rights Management Services (RMS)
- X.400 support

SP1 brings a wealth of new features and enhancements for Exchange messaging architects, administrators, and end users.

To improve Edge Transport server management, SP1 adds a Server parameter to the Start-EdgeSynchronization cmdlet so that administrators can run the cmdlet from a remote computer. The Test-EdgeSynchronization cmdlet has been enhanced so that results on subscription status for individual users can be verified. The cloned configuration scripts have been improved so that cloning of configuration information, server deployment, and backup and restore are optimized for environments that use multiple Edge Transport servers.

UM Server Role Enhancements

To increase interoperability with Office Communications Server (OCS) 2007, SP1 enhances the UM server role significantly. Some of the new features you'll get when using SP1 and OCS 2007 together include:

- a New Dial Plan wizard to create E.164 and Session Initiation Protocol (SIP) Uniform Resource Identifier (URI) dial plans
- new logic for resolving calling numbers
- forwarding notification when leaving voice messages
- high-fidelity voice message recording
- PIN-less access to Outlook Voice Access from Office Communicator
- subject and priority association in Communicator
- media stream firewall traversal
- missed call notification integration in Communicator
- prohibiting play on calls with Communicator that are subject to call forwarding rules
- the ability to properly handle incoming fax calls from OCS

Even without OCS 2007, SP1 offers UM improvements such as support for Secure Real-time Transport Protocol (SRTP), configuration of Mutual Transport Layer Security for dial plans through Exchange Management Console, the Enable UM wizard for adding SIP or E.164 addresses for users, modification of extension numbers and SIP or E.164 addresses for UM users through Exchange Management Console, fax tone detection, and Quality of Service support.

A Host of Additional Features

SP1 has many other improvements in addition to the major enhancements I've described. Although perhaps not as dramatic, these features will undoubtedly be warmly received by Exchange administrators.

Move Mailbox. Move Mailbox has been a favorite feature of Exchange administrators for years. Exchange 2007 greatly improved Move Mailbox by adding Exchange Management Shell scripting capabilities, and SP1 brings yet more improvements.

With SP1, an administrator can export mailbox content to a PST file by using the PSTFolderPath parameter with the Export-Mailbox cmdlet. You can combine this operation with other parameters to filter content or export multiple mailboxes. Clearly, this functionality is useful for data migration operations that would otherwise be limited by bandwidth restrictions, or in support of e-discovery requests for litigation.

Exchange ActiveSync. EAS has received improvements geared for both administrators and end users. When the Client Access server role is configured on a server with SP1, a default EAS policy is created. Any users without

an EAS policy will have this new default policy applied. This change means administrators no longer have to explicitly apply a default policy to new EAS users. Administration requires less effort and you'll have better security for your environment.

New EAS policy settings are also available. With these new policies, administrators can enforce encryption of main memory contents on the remote device; disable removable storage capability; disable POP3, IMAP4, Short Message Service (SMS), and Message Management System (MMS) capability; block applications; or disable Wi-Fi, Bluetooth, or infrared capabilities on mobile devices. This kind of device control greatly enhances security. However, note that some of these features aren't supported on Windows Mobile 6.0, and some require the Exchange 2007 Enterprise CAL. To use the full suite of features enabled by EAS in SP1, the bottom line is that you'll need to invest in new devices that aren't available yet and won't be until Microsoft and OEMs introduce devices that run Windows Mobile 6.1.

In addition, the remote wipe capability now offers a confirmation option before a mobile device is reinitialized, and Direct Push functionality has been improved by reducing the amount of data that is sent and received by the device.

POP3 and IMAP4. Exchange Management Console has been enhanced to provide a new administrative interface for POP3 and IMAP management; previously, these functions were available only through Exchange Management Shell. You'll find the interface by navigating to Client Access under Server Configuration in the console tree, clicking either the POP3 or IMAP4 tab, then selecting Properties.

Exchange Web Services. With the big developer push toward Web services in Exchange, it's encouraging to see that Exchange Web Services now includes access to and manipulation of Public Folders, management of delegates and access to delegate resources, permissions management, and identifier translation.

Public folders. Despite public folders being de-emphasized in Exchange 2007, many organizations continue to use them. SP1 has brought some necessary management improvements. Administrators will welcome the Public Folder Management Console as a means to create and manage public folders via Exchange Management Console. You can also manage public folder referrals via the Properties tab of a pubic folder database in Exchange Management Console. In Exchange 2007 RTM, you have to use Exchange Management Shell to perform these actions, but SP1 gives you a choice. Another boon to administrators is the addition of a new administrator role called Exchange Public Folder Administrator that you can use to granularly delegate Public Folder management.

For end users, mail-enabled public folders now appear when previewing membership of address lists, address policies, and Distribution Groups—including dynamic ones.

Mailbox management. SP1 introduces bulk mailbox creation through Exchange Management Console when you select multiple existing user accounts. You also get two new wizards: the Manage Full Access Permission wizard, which lets you grant or remove Full Access permission for a mailbox; and the Manage Send As Permissions wizard, which lets you grant or remove Send As permissions.

Messaging records management. To establish some level of parity with the Mailbox Manager feature of Exchange 2000 Server and Exchange Server 2003, SP1 lets you apply messaging records management (MRM) policies to managed default folders (e.g., Inbox) even with the Standard version of Exchange. For managed custom folders, each mailbox that uses MRM must have an Exchange Server Enterprise CAL.

Defragmentation monitoring. A minor but perhaps useful addition for administrators is the extended information for Event 703, which can help you monitor online defragmentation pass completions. With Exchange 2007 RTM, such monitoring is a cumbersome process that requires analyzing the event log and matching Event 700 and Event 703 messages to determine how successful online defragmentation attempts have been over time. With SP1, all the information you need—and more—is contained in Event 703. Figure 1 shows an example of the enhanced text.

Performance Monitor has received two new Extensible Storage Engine (ESE) performance counters that also monitor the effectiveness and efficiency of online defragmentation: Instances\Online Defrag Pages Freed/Sec shows the number of pages freed per second as a result of online defragmentation, and Instances\Online Defrag Data Moves/Sec shows the number of times per second that data is moved from one page to another during online defragmentation.

```
MSExchangeIS (19052) SG05: Online defragmentation has
completed the resumed pass on database 'e:\MDB05\
database5.edb', freeing 42794 pages. This pass started
on 6/16/2007 and ran for a total of 124919 seconds,
requiring 7 invocations over 4 days. Since the
database was created it has been fully defragmented 14
times over 73 days.
```

Figure 1: Extended Event 703 text in Exchange 2007 SP1

Transport dumpster. SP1 uses an enhanced transport dumpster process to support lossy recoveries in an LCR environment. In Exchange 2007 RTM, the transport dumpster is automatically exploited during a CCR recovery; the Restore-StorageGroupCopy cmdlet has been updated in SP1 to include a call to the transport dumpster in LCR recovery to provide messages that might have been lost as a result of the failure of the storage group in question.

Exchange Management Console. SP1 offers a new Manage Clustered Mailbox Server wizard that provides the same functionality as the Move-, Stop-, and Start-ClusteredMailboxServer cmdlets. And there are new controls in Exchange Management Console that have the same functionality as the Suspend-, Resume-, Update-, and Restore-StorageGroupCopy cmdlets.

Dramatic Advances with SP1

SP1 brings a wealth of new features and enhancements for Exchange messaging architects, administrators, and end users. Some are just nice-to-have improvements, but others, such as SCR, can have a much more dramatic effect on the design and deployment of your messaging environment. To get the best out of these new improvements, you should spend some time investigating what all of these new changes can do for your environment.

InstantDoc ID 97606

Kieran McCorry

(kieran.mccorry@hp.com) is a distinguished technologist in the HP Services Advanced Technology Group, a Microsoft MVP, and a Microsoft Certified Architect. He works with the planning, design, and implementation of messaging infrastructures. He's the author of four books on Microsoft Exchange Server.

WINDOWS VISTA AND SERVER 2008

GROUP POLICY ENHANCEMENTS

NEW FEATURES FOR GPOs AND GPMC

BY DARREN MAR-ELIA

Now that Windows Vista has shipped and Windows Server 2008 is nearing release, it's a good time to look more closely at some of the Group Policy enhancements these new versions of the OS introduce. Group Policy has taken on an important role as the key configuration management mechanism within Windows. That's a good thing. It's challenging though, because more enhancements mean more options, more options mean more choices, and more choices mean more complexity. The good news is that the enhancements Microsoft is making in Group Policy Management Console (GPMC) for Server 2008 will mitigate some of these complexities.

Group Policy Client Service

There are significant changes to some of the unseen aspects of Group Policy. Most importantly, the Group Policy engine has been moved out of the system Winlogon process, where it has run ever since Windows 2000, and into its own Group Policy Client service. The Group Policy Client service is a nonrestartable service in Vista and Server 2008 that runs the Group Policy processing engine. It runs outside of Winlogon and provides an isolated environment for Group Policy client-side extensions (CSEs) to run in. In fact, it even provides isolation between Microsoft CSEs and third-party ones, so if a third-party CSE crashes, Microsoft's CSEs will not be affected during Group Policy processing.

Slow Link Detection

The slow link detection process in Group Policy has also changed. If you're familiar with slow link detection in previous versions of Windows, you know that, at the beginning of each Group Policy processing cycle, a client uses Internet Control Message Protocol (ICMP) to ping its Active Directory (AD) domain controller (DC) to determine its availability and compute the speed of the link between the client and DC. If this process fails for any reason (e.g., if ICMP is blocked or restricted by the network or if the DC is unavailable over ICMP), then Group Policy processing fails. Additionally, the calculation used for slow link detection was relatively crude and often resulted in a slow link being detected for no good reason.

In an effort to improve this process, Group Policy now leverages the new version of the Network Location Awareness (NLA) service provider that ships with Vista and Server 2008. NLA checks whether the DC is available and, if it is, determines the speed of the network link between client and DC. It uses robust protocols, such as remote procedure call (RPC), instead of the relatively simple and often-blocked ICMP. This results in better slow link detection and the ability to quickly determine whether a DC is available. As it turns out, whether or not a DC is available constitutes a very important factor in the next new feature I'll talk about, namely the NLA-based refresh of Group Policy.

NLA Background Refresh

In addition to using NLA to improve slow link detection, the Group Policy engine relies on NLA to improve the background Group Policy update process. In Windows versions up to and including Vista and Server 2008, a background refresh occurs every 90 minutes on workstations and member servers. Plus, there's an additional refresh of up to 30 minutes in a randomized value that ensures all systems don't refresh at once. Say a laptop's background refresh occurred while a user was travelling home with it on the train. Because the DC wasn't available, the refresh would simply fail. Ten minutes later, when the user is home and has plugged into the corporate VPN, the DC is available, but depending upon when the last refresh occurred, it may be many minutes before the next Group Policy update via background refresh.

NLA provides a new kind of background refresh for Group Policy in Vista and Server 2008. If a system running one of these new versions of the Windows OS attempts to refresh Group Policy in the background and fails because the DC isn't available, then the next time the DC becomes available, the client triggers a background Group Policy refresh as soon as NLA detects the DC. The NLA refresh appears in the new Vista Group Policy Operational log, as shown in Figure 1.

The NLA refresh can be useful when you're trying to push out a new policy to affect some behavior on your client machines and you don't want your users to wait for more than an hour after they get back on the network to receive the change. However, it's important to note that this feature works only if the previous background refresh attempt failed.

Multiple Local GPOs

How many times have you wished you could set a local GPO on your Windows XP systems that wouldn't affect administrators logging onto those systems or that applied only to a specific user on the local system? Multiple local GPOs in Vista and Server 2008 are the answer you've been waiting for. As the name implies, multiple local GPOs provide a way of having more than one local GPO on a given Windows system. Systems prior to Vista store the local GPO in the file system under C:\windows\system32\grouppolicy. On Vista and Server 2008 systems, the default local GPO still exists in that location, but you can also create three new types of local GPOs:

- A non-administrator local GPO lets you define user-specific policy settings that apply only to any non-administrative user (such as a user who's not a member of the local Administrators group) logging onto the computer.
- An administrator local GPO lets you define user-specific policy settings that apply only to any member of the local Administrators group logging onto the computer.
- A user local GPO lets you define user-specific policy settings that apply only to a particular local user account defined on the workstation or member server. This policy doesn't apply to domain accounts.

These new local GPOs are stored in folders based on the SID of the group or user to whom they apply, under C:\windows\system32\group policy users. In Windows OSs before Vista, Group Policy processing has an order of precedence that starts with the local GPO, then site-linked GPOs, then domain-linked GPOs, and finally organizational unit (OU)-linked GPOs. When a user logs on, Windows applies the User Configuration portion of Group Policy. The order of precedence with multiple local GPOs on Vista and Server 2008 is

1. Default local GPO
2. Non-administrator or administrator local GPO (if any)
3. User local GPO (if any)
4. Domain-based GPOs (site, domain, and OU-linked)

How do you get to those multiple local GPOs on your Vista or Server 2008 system? Here are the steps you need to take to be able to edit the other local GPOs:

1. From the Start menu, choose Run, then

Learning Path

WINDOWS IT PRO RESOURCES

"How can I manage Group Policy for Windows Vista machines?" InstantDoc ID 95128

"Managing Windows Vista Group Policy Options," InstantDoc ID 94926

"Converting an ADM File into an ADMX File," InstantDoc ID 97123

"Network Access Protection in Windows Server 2008," InstantDoc ID 95617

MICROSOFT RESOURCES

Windows Server Group Policy
technet.microsoft.com/en-us/windowsserver/grouppolicy/default.aspx

Group Policy ADMX System Reference Guide
microsoft.com/downloads/details.aspx?FamilyID=b0628355-baa2-4565-80a4-467245db9e28&DisplayLang=en

ADMX Migrator
microsoft.com/downloads/details.aspx?familyid=0F1EEC3D-10C4-4B5F-9625-97C2F7310900C&displaylang=en

Group Policy Log View
microsoft.com/downloads/details.aspx?FamilyID=bcfb1955-ca1d-4f00-9cff-6f541bad4563&DisplayLang=en

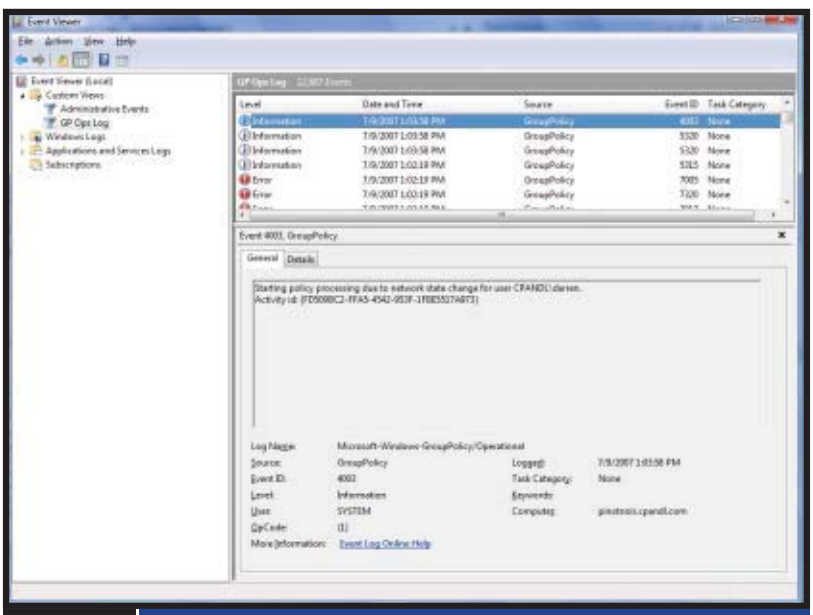


Figure 1: An NLA refresh event in the Group Policy Operational log

type mmc to launch a blank Microsoft Management Console (MMC). (Because running MMC requires elevated privileges, when User Account Control—UAC—is enabled, you'll be prompted for credentials.)

2. In MMC, choose File, Add/Remove Snap-in and scroll down to Group Policy.

3. Select Add to add that snap-in to the console, and browse to the GPO you want to edit. The default is Local Computer, which refers to the default local GPO. However, at this point, click the Browse button to see other options.

4. In the *Browse for a Group Policy Object* dialog box, select the Users tab. You'll see something similar to Figure 2. At this point, you can choose a specific local user, the general administrator, or the non-administrator and click OK to load the associated local GPO into the MMC Group Policy editor (GPE) snap-in for editing.

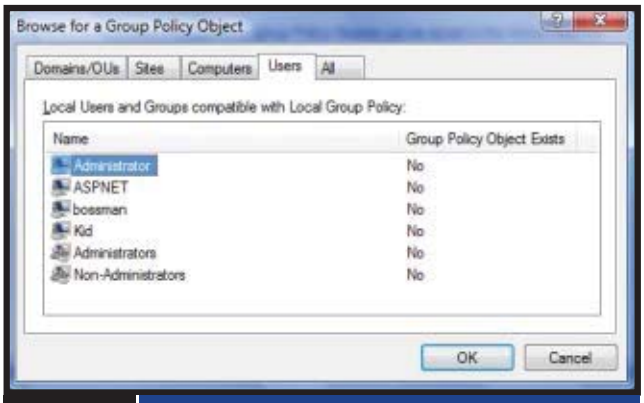


Figure 2: Locating a local GPO in Vista

Figure 2 is a snapshot of my system; it lists several local users, plus Administrator, Administrators, and Non-Administrators. None of these local GPOs yet exists. But if I use the above instructions to add one of them to GPE and make modifications to it, it will exist within the local file system in the C:\windows\system32\GroupPolicyUsers folder.

ADMX Templates

You might have heard that the format for Administrative Templates, or ADM files, has changed in Vista and Server 2008. ADM files create the policy options you see under the Administrative Templates nodes in GPE. ADMX files in Vista perform the same role, but you won't be able to work with them the same way. For example, if you created custom ADM files with Notepad or your favorite text editor, you'll find it difficult to do the same thing with the new ADMX files. That's because Microsoft has adopted a new XML data format for ADMX files, and their partners, ADML files. (Each ADMX file puts language-dependent string references in an ADML file for that specific language.)

It's easiest to explain the new ADMX by looking at it side-by-side with the old ADM. Table 1 compares the two technologies.

As you can see in Table 1, there are plenty of differences between ADM and ADMX. A major difference is storage—having a central store for ADMX files versus storing the same ADM files in every GPO on every DC (the so-called "SYSVOL bloat" problem). The central store (aka central or domain-wide repository) is simply a folder called PolicyDefinitions that you create manually in the \\<domainName>\SYSVOL\<domainName>\Policies folder on your DC. You then copy the contents of C:\Windows\PolicyDefinitions from one of your Vista or Server 2008 systems into this newly created folder and, voila, you've created the central store.

I've created a free utility at www.gpoguy.com/cssu.htm that you can use to automate the central store creation and population process. Once the central store is created and populated, both GPE and GPMC, running from Vista or Server 2008, will recognize its existence and reference ADMX files from that location instead of locally.

Another advantage to the new ADMX format, that I alluded to earlier, is the separation of the language-specific strings in new ADML files from the portion of the template that defines the policy settings. This lets you use one set of ADMX files for each supported language, and the ADML file for your local language is used whenever you launch GPE. So, instead of having to maintain multiple, language-specific ADM files as in the past, this new format lets you easily support editing of Administrative Template policy in multiple languages.

You can convert your custom ADM files to ADMX files by using a free ADM to ADMX converter that Microsoft provides. This tool, called the ADMX Migrator, also makes creating ADMX files from scratch a cinch. For download information, see "ADMX Migrator" in the Learning Path.

Interoperability

Before I look at problems arising in the mixed environment of Vista with ADMX, and Win-

Table 1: Comparing ADM and ADMX

Feature	ADM (Pre-Vista OSs)	ADMX (Vista and Server 2008)
Default location of template files	C:\Windows\inf	C:\Windows\PolicyDefinitions
Storage of template files	Stored with the GPO in SYSVOL and replicated to all DCs.	Stored locally on the machine editing the policy or in the new central store in the SYSVOL area of the DC but not in each GPO.
Language Independence	ADM files embed strings into the file, thus requiring a different version of an ADM for each language.	ADMX files put language-dependent string references in a separate ADML file. Each ADMX has exactly one corresponding ADML for each language. ADML files are stored in a language-named folder under the C:\Windows\PolicyDefinitions folder or in the central store.
Updating template files	When new ADMs are found in C:\Windows\inf, they are, by default, copied to the GPO being edited.	ADMX files are never copied into the central store automatically. The central store must be populated manually.
Syntax of template files	ADM files use a proprietary language that has been around since Windows NT Server 4.0.	ADMX files use a language similar to ADM, but it's wrapped in XML and thus looks completely different. For more information about these differences, see "Converting an ADM File into an ADMX File," in the Learning Path.
Number of files shipped with the OS	Seven ADM files ship with XP SP2. Five of those are used when creating new GPOs.	One hundred thirty-two ADMX files and their companion ADML files ship with Vista. As of this writing, Server 2008 includes 145 ADMX/ADML files.

dows XP or Windows Server 2003 with ADM, I want to emphasize that these are problems for administrators. For GPO application on clients (of whatever type), the ADM or ADMX templates aren't relevant. The templates are used only for the administrative view of the GPOs and are for administrative tasks, such as working with specific settings. The actual settings applied via GPO are still stored in registry.pol and related files, which didn't change in Vista and Server 2008. This means that a GPO created and managed via either Vista or Server 2008 is perfectly compatible with downlevel clients for settings they support.

Administrators need to know that XP, Server 2003, and Win2K can't "see" ADMX files. Thus, if you create a GPO and set some Vista-specific Administrative Template policies from GPE running on Vista, then try to edit that GPO from GPE running on XP, you won't see the Vista-specific settings because they're in Vista ADMX files that the XP machine can't read. A further complication is that XP and Vista don't store their template files the same way.

Let's take the following mixed-environment scenario. Suppose you create a new GPO on your Vista workstation. Let's also suppose that you've created the central store, so all GPOs managed from Vista are referencing the ADMX files from that central location. (Remember, Vista no longer stores template files in the SYSVOL portion of each GPO.) Now you edit that new Vista GPO on your XP machine. XP looks in the SYSVOL portion of that GPO and notices that there aren't any ADMs there, so it copies its own ADMs into SYSVOL and pollutes your brand new Vista GPO.

How can this tragic scene be avoided? I count at least three ways. First, after you introduce Vista into your environment; you can make a plan to edit GPOs only from Vista systems. This guarantees that all GPOs from that time forward will see all settings. Second, you can keep your environments separate. If you have some XP and some Vista systems, manage the GPOs that apply to XP from XP systems and the ones that apply to Vista from Vista systems. However, if you absolutely, positively must manage your Vista GPOs from downlevel systems, consider the third option, which is to enable the following policy on users who edit GPOs from XP, Win2K, and Server 2003 systems. This policy will prevent the downlevel platforms from automatically updating the SYSVOL portion of your clean Vista GPOs with ADM files every time you edit them:
User Configuration\Administrative Templates\System\Group Policy\Turn off automatic update of ADM files

Better Logging

A big challenge of Group Policy troubleshooting in XP and Server 2003 environments is getting useful information out of the logs generated during a Group Policy processing cycle. It's especially true if you try to make sense of the userenv.log file, located in %WINDIR%\Debug\Usermode, a cryptic text log used by both user profiles and Group Policy to log the details of their activities. The good news is that Microsoft moved away from the userenv.log file in Vista and Server 2008. GPO processing now runs outside of Winlogon and leverages its own service. So instead of the userenv.log file, detailed trace information about Group Policy processing is found in the Group Policy Operational log. This log, shown in Figure 3, contains step-by-step detail of Group Policy processing on a given system.

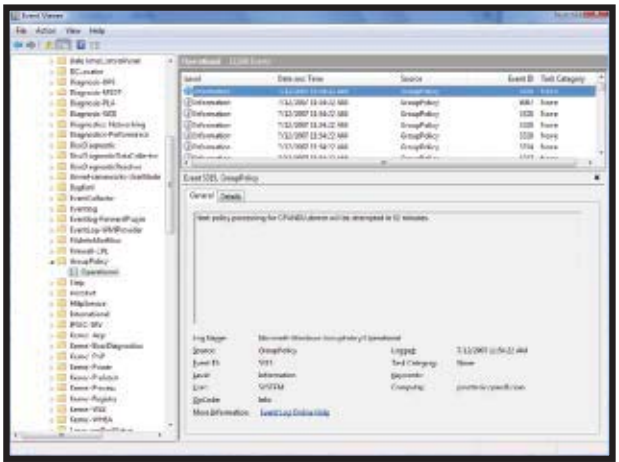


Figure 3: Viewing the Group Policy Operational log

You can locate the Group Policy Operational log in the new Event Viewer by expanding the Applications and Services Logs node and then clicking Microsoft, Windows, GroupPolicy, Operational. Note that the new eventing system (code-named Crimson) in Vista and Server 2008 allows you to do interesting things such as forward specific events to a central collection point (called subscribing to events) or create filtered views of specific events. In addition to the Event Viewer, Microsoft has provided a free command-line tool called GPLogView that lets you output Group Policy Operational log events to text or HTML files. For download information, see "Group Policy Log View" in the Learning Path. If you like writing code, you can download the source code for GPLogView and contribute changes and enhancements to it at www.codeplex.com/gplogview.

New Policy Areas

In addition to all the core changes to Group Policy in Vista and Server 2008, Microsoft has added some new configuration capabilities. I don't have room to discuss them all here, so I'll just highlight some of the more interesting ones.

Deployed printers. In a move that's similar to providing the printer deployment capability in Server 2003 R2, Microsoft has finally made deployed printers full citizens in the Group Policy world. Vista and Server 2008 systems can process either per-computer or per-user deployed printer definitions to allow you to map printers for computers and users within Group Policy. (Note that this capability can also be leveraged by XP or Server 2003 systems, but the mechanism to trigger evaluation of the printer policies via startup/logon script is different.) This capability requires an AD schema update if you're not running the R2 (or later) version of the AD schema. The LDAP Data Interchange Format (LDIF) schema files that support this feature (and others) can be found on the Vista CD-ROM in the sources\adprep folder. If you're running the Server 2008 AD schema, then these additions are already included. Deployed Printers are located within the Group Policy namespace under Computer (or User) Configuration\Windows Settings\Deployed Printers.

Power management. Vista and Server 2008 finally let you control power management features via Group Policy. These include choosing the default power plan for a system and configuring every aspect of when a system sleeps, hibernates, or shuts down. You can find most of the power configuration options at Computer Configuration\Administrative Templates\System\Power Management, but you can also set a per-user option to require a password when a system comes out of hibernation or standby by setting the policy at

User Configuration\Administrative Templates\System\Power Management.

New security policies. Vista and Server 2008 adds quite a few new security policy capabilities to the mix. Several are highlighted here:

- *Wired and Wireless Policy*—New for Vista and Server 2008 is the support for setting wired network security policy. Wired policy applies to Ethernet network links and lets you enforce 802.1x usage on those links for machines on your network. Wireless policy updates the policy supported in XP and provides new support for enhanced encryption schemes, such as Wi-Fi Protected Access 2 (WPA2), as well as the ability to explicitly deny or allow access to certain Service Set Identifiers (SSIDs). (Note that some of these capabilities are available only to Vista and Server 2008 systems.) Find the Wired and Wireless Policy in Group Policy under Computer Configuration\Windows Settings\Security Settings.
- *Windows Firewall with Advanced Security*—This new area within Group Policy is actually a redesign of two previously supported policy areas—IPsec and Windows Firewall. The new UI makes it simpler for you to define Windows Firewall exceptions as well as implement IPsec filtering on your network. Older IPsec and Windows Firewall policy settings are still available for backward compatibility, but you should use this new Group Policy area to control network security on your Vista and Server 2008 devices. Find this capability in Group Policy under Computer Configuration\Windows Settings\Security Settings.
- *Network Access Protection (NAP)*—This policy area supports the new NAP features in Server 2008 and lets you use Group Policy to configure client NAP behavior on your network. Find this capability in Group Policy under Computer Configuration\Windows Settings\Security Settings.

Device restrictions. Device restriction support, and the ability to manage it via Group Policy, is probably one of the more compelling features for deploying Vista. The Device Restrictions policy in GPE lets you control access to any number of removable storage devices. Not only can you control which devices can be used, but you can also specify whether a user can read or write from a removable device. Figure 4 shows the options that are available for this policy area. You can set this policy either per-computer or per-user and you can find it under Computer (or User) Configuration\Administrative Templates\System\Removable Storage Access.

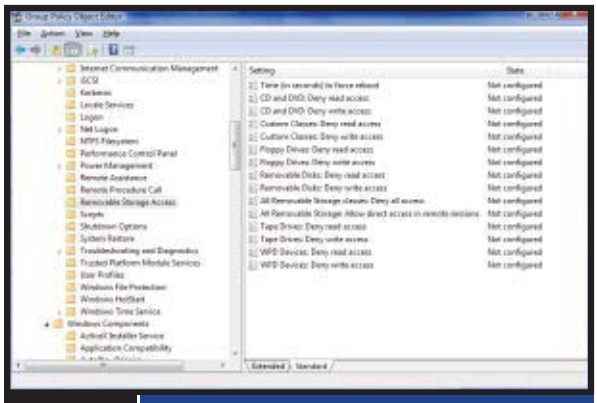


Figure 4: The Group Policy removable storage restriction options

GPMC Changes in Server 2008

There are a number of new GPMC changes coming in Server 2008. You'll be able to search through Administrative Template settings within GPOs for, among other criteria, all enabled or disabled policies with a certain keyword in the policy, for Explain Text, for the Supported OS tag, or for whether the policy is managed or is a "preference." You can also use search filters to filter the view of settings that appear in GPE.

The ability to create per-GPO and per-setting comments is also new. Those comments are stored with the GPO and provide a way for you to let others know what a particular GPO or setting is used for.

Now you'll have the ability to provide new Starter GPOs. Starter GPOs are really collections of Administrative Template settings that you can apply to live GPOs. Starter GPOs let you create, for example, a group of Administrative Template settings for desktop lockdown that you can re-use whenever you create a new desktop lockdown GPO. Note that Starter GPOs support only Administrative Template policy but provide a quasi-offline capability for defining GPO settings that aren't immediately live. You can also include Starter GPOs in Resultant Set of Policy (RSoP) modeling calculations so that you can see the impact that applying a Starter GPO to an existing live GPO has on your users and computers.

Microsoft added a very important set of new policy capabilities called Group Policy preferences in time for the release of Server 2008. Group Policy preferences is the name given to the former DesktopStandard PolicyMaker Standard Edition and PolicyMaker Share Manager products that Microsoft acquired in 2006. These new Group Policy extensions supply the missing link for providing coverage of almost every desktop and server configuration scenario imaginable. Group Policy preferences supports clients from XP forward and adds new Group Policy features such as support for mapped drives (without having to write scripts), distribution of shortcuts, power management, device restrictions, and local user and group management, to name just a few.

Time to Upgrade?

Overall, Vista and Server 2008 add some truly compelling features to the manageability and capability of Group Policy as the configuration management technology for Windows. Finally, you can map printers, manage power settings, and control removable storage access natively in Windows. These are all features that used to require third-party products to manage. The catch, of course, is that you need to upgrade your clients to Vista to take advantage of some of these desktop features. Even so, Group Policy still doesn't provide all of the features you need. For example, you still need to purchase a product like Microsoft's Advanced Group Policy Management in order to get change management for your Group Policy environment, and Group Policy still has no built-in enterprise reporting capability.

That said, if you are looking for justification to upgrade, the cost savings and risk mitigation that the many new features provide might be enough. In any case, these new features show that Microsoft is committed to making Group Policy an important part of your Windows management toolset.

InstantDoc ID 97623

Darren Mar-Elia

(dmarelia@windowsitpro.com) is a contributing editor for *Windows IT Pro* and is CTO and Founder of SDM Software. He maintains a Group Policy resource Web site (www.gpoguy.com) and is coauthor of *Microsoft Windows Group Policy Guide* (Microsoft Press).

3 Info-packed eLearning seminars

EXCHANGE 2007 Mastery Series

Hosted by Windows IT Pro

for $99!

WHEN
January 28, 2008 – 11:00 AM EST

WHERE
On your computer

COST
$99/registrant for 1, 2 or all 3 live online sessions (includes access to all archived versions)

SESSIONS
Planning for Archiving & Compliance

Optimizing Your iSCSI Network Storage

Memory vs. Spindles – Finding the Sweet Spot

RESERVE A SEAT by going to:
www.windowsitpro.com/go/elearning/masteringexchange2007

SPEAKER
Mark Arnold

MCSE+M, Microsoft MVP

Mark Arnold is a senior technical architect for Anix, a UK-based storage integrator, where he solves storage and compliance problems for his clients by using Microsoft Exchange as a key component in SAN and NAS deployments. He's also a regular contributor to Microsoft's "Industry Insiders" TechNet program and is active on Exchange newsgroups and forums.

ABOUT THE SESSIONS

Planning for Archiving & Compliance

Managed folders and journaling may not be enough as your organization grows. Learn how to combine Exchange's built-in features with tiered storage to delay, or possibly even eliminate, the need for a third-party archiving solution.

Optimizing Your iSCSI Network Storage

With Exchange 2007 storage, you need to answer some key up-front questions: Will you use fewer servers, or the same? Larger disks, or more small ones? We'll examine LUN layouts to learn how to optimize iSCSI for Exchange 2007.

Memory vs. Spindles – Finding the Sweet Spot

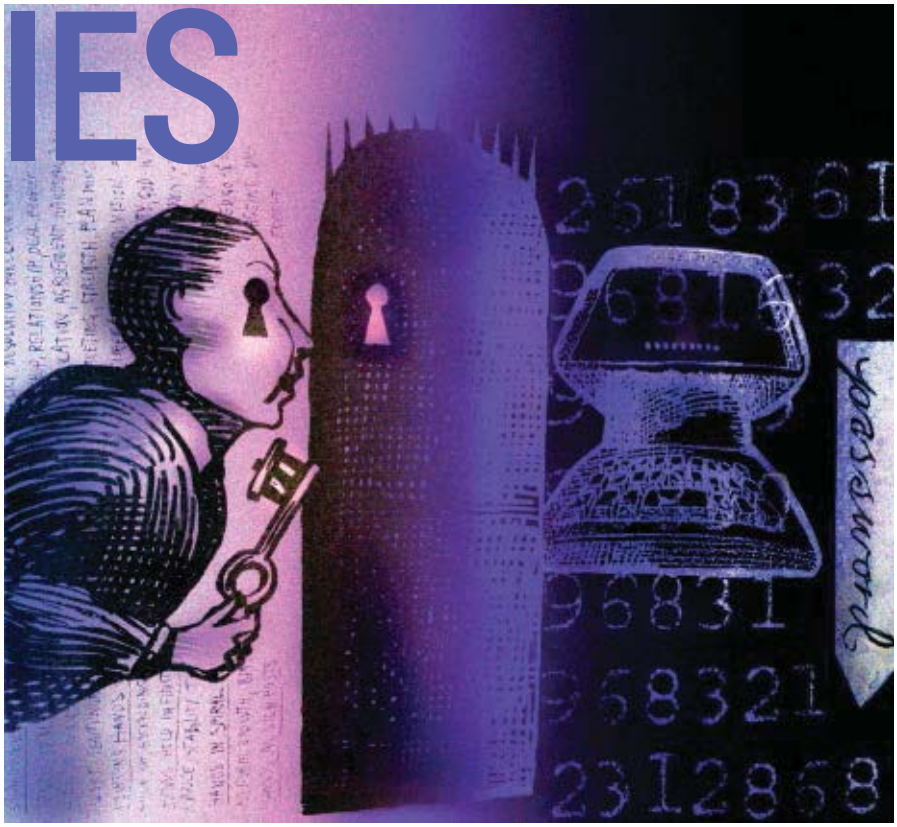
Exchange 2007 requires more memory than Exchange 2003... but where's the sweet spot? When do you stop adding memory and let disk spindles handle the remaining load? I'll show you how to turn Microsoft's guidelines into real-world server configurations.

REGISTER TODAY — seats are limited,
to allow lots of live Q&A at the end. (Questions can also be submitted after the session, by email.)

For more information, or to register, go to:
www.windowsitpro.com/go/elearning/masteringexchange2007

Windows IT Pro

WINDOWS SERVER 2008 PASSWORD POLICIES



The new Server OS resolves earlier password policy limitations

One of Windows' most important security policies that every Windows administrator is certainly familiar with is the password policies. These policies let you enforce password quality requirements (e.g., minimum password length, maximum password age) for the passwords of local or domain user accounts. As you might know, Windows Server 2003 and Windows 2000 Server password policies have some important limitations. In this article I explain these limitations and discuss how Windows Server 2008—Microsoft's upcoming Server OS—resolves them. I also explain how you can configure and use Server 2008's password policies. At press time, Microsoft had released Server 2008 Release Candidate 0 (RC0) and was planning to launch the Server OS on February 27, 2008.

A Flexible Solution for a Serious Problem

A serious limitation of the password policies in Windows 2003 and Win2K is that administrators can define only one password policy that applies to all user accounts in a domain. You can define this global domain password policy from the Default Domain Policy Group Policy Object's (GPO's) Password Policy settings or from any other GPO that's linked to the Active Directory (AD) domain object. To access the Password Policy configuration interface, go to the \Computer Configuration\Windows Settings\Security Settings\Account Policies GPO container. Even though you can define different password policies in the GPOs and link them to AD organizational units (OUs) or computer accounts, these password policies don't apply to domain accounts—instead, they apply to the local accounts that are defined in the security databases of the computer accounts to which the GPOs apply.

Organizations typically want to impose different password quality requirements for certain categories of domain accounts. A classic example is having a different password policy for administrator accounts and regular user accounts. The security rationale is simple: Administrator

Jan De Clercq
(jan.declercq@hp.com) is a member of HP's Security Office and focuses on identity management and security in Microsoft products. He is coauthor of *Microsoft Windows Security Fundamentals* (Digital Press).

Illustration by Todd Davidson / images.com

accounts have more powers (permissions and rights) than plain user accounts, so you might want a higher quality authentication process for administrators than for regular users. Another way to provide stronger authentication is to enforce the use of smart card logon for administrator accounts.

Windows 2003 and Win2K provide two workarounds for organizations that want to define different passwords policies in a single domain, although both workarounds are difficult to implement. One workaround is to deploy separate domains for each of the account categories that you want to define a special password for. The other workaround is to develop a special "password filtering" DLL that you then deploy to all your domain controllers (DCs). The second solution is rarely used because it's even more complex and time consuming than the first solution.

Server 2008 comes to the rescue by introducing fine-grained password policies that let administrators define different password policies for different domain account categories in a single domain. This new fine-grained password policy functionality can be applied only to domain accounts—not to local accounts.

Server 2008 introduces the same functionality for the account lockout policies that in earlier Windows Server versions were crippled by the same limitation (i.e., you could define only a single account lockout policy for all domain accounts). Account lockout policies ensure that user accounts automatically become unusable after a user enters a certain number of incorrect passwords. The administrator must define a bad password threshold to configure the account lockout policy.

Configuring Fine-Grained Password Policies

Configuring Server 2008's fine-grained password policies is entirely different from defining the classic domain account or local account password policy in earlier Windows versions (which I described previously). You can't use GPO settings to configure fine-grained password policies, because Microsoft uses a different (non–GPO-based) mechanism to store and enforce these policies.

Server 2008's fine-grained password policies are stored in a new AD container called the AD Password Settings Container, which is located in the System container of the AD domain naming context. To define a new fine-grained password policy, you must create a new AD object of the msDS-PasswordSettings object class in this container. Objects of this class are referred to as Password Settings objects (PSOs) in the Microsoft documentation. By default, only members of the Domain Admins group can create PSOs, because only members of this group have the AD Create Child and Delete Child permissions on the Password Settings Container. (I discuss the tools you can use to create and configure PSOs in a later section.)

To apply the PSOs you created, you must link the PSO to an AD user or group object. To do so, you don't need permissions to the AD object itself; you simply need Write permissions on the PSO. By default, only members of the Domain Admins group have this permission. Therefore, only members of the Domain Admins group can link a PSO to a group or user—although you can obviously delegate these permissions to other administrators.

Table 1 summarizes the attributes that are linked to Server 2008 PSOs. Note that a PSO can store not only password policy settings but also account lockout policy settings. Remember that Server 2008 supports both fine-grained password and account lockout policies. Two important PSO attributes are the msDS-PSOAppliesTo and msDS-PasswordSettingsPrecedence attributes.

The msDS-PSOAppliesTo PSO attribute is a multi-valued attribute that determines what AD user accounts or groups the PSO will be linked to. Even though password and account lockout policies can be linked to any AD user, group or computer object, or OU, PSOs are effective only for the user accounts and global groups they are linked to. In addition, PSOs are effective only if your AD domain is in the native Server 2008 domain functional level—which means that all the DCs in your domain must be running Server 2008.

The msDS-PasswordSettingsPrecedence PSO attribute holds an integer value that is used to resolve conflicts if

Table 1: Important AD PSO Attributes

Attribute Name	Required?	Description	Example Value
cn	Yes	Common name	MyPasswordPolicy
msDS-PasswordSettingsPrecedence	Yes	Password settings precedence	10
msDS-PSOAppliesTo	No	Multi-valued attribute that holds the DNs of the objects that a PSO applies to	CN=Joe,CN=Users, DC=dc,DC=net
Password Policy-Related Settings			
msDS-PasswordReversibleEncryptionEnabled	Yes	Password reversible encryption status	TRUE
msDS-PasswordHistoryLength	Yes	Password history length	24
msDS-PasswordComplexityEnabled	Yes	Password complexity status	TRUE
msDS-MinimumPasswordLength	Yes	Minimum password length	6
msDS-MinimumPasswordAge	Yes	Minimum password age in days	5
msDS-MaximumPasswordAge	Yes	Maximum password age in days	30
Account Lockout Policy-Related Settings			
msDS-LockoutThreshold	Yes	Lockout threshold	0
msDS-LockoutObservationWindow	Yes	Observation window for lockout of user accounts in minutes	30
msDS-LockoutDuration	Yes	Lockout duration for locked out user accounts in minutes	30

Securing the Desktop Infrastructure

Security of the desktop infrastructure is your first line of defense. Making sure that users have a well-managed and secure workstation can mitigate support costs, protect your organization's data, and keep users productive by protecting against malware and anti-virus threats. The resources in this learning path will show you the tools and technologies that Microsoft offers to help keep your desktop infrastructure secure.

Register today:
www.microsoft.com/technet/security/learning

Learning Paths for Security

Critical Security Information for IT Professionals

Learning Paths for Security is an online security curriculum where IT professionals can access the latest in security technology information, from the next big thing to how to solve today's security issues. Information is arranged by topic, technical depth (Level 100 through 400), and stage of the security lifecycle, so it's easy to find the information applicable to your specific situation and level of knowledge.

GUIDES
Download and print these white papers, resource kits, and articles to read and save for reference.

WEBCASTS
From Q&A sessions with experts on Microsoft® technology, the industry or both; to technical and product demos, these 60-90 minute broadcasts are available online so you can watch at any time, from any place.

ONLINE SEMINARS
These compilations of materials from a live event (including presentations, videos, and tools) are a quick way to get up-to-date on a topic of interest.

VIRTUAL AND HANDS-ON LABS
Test Microsoft software and servers in a sandbox environment.

TOOLS
Download free applications or software programs to help accomplish specific tasks you need to complete.

Learning Paths for Security can be found at:

www.microsoft.com/technet/security/learning

Microsoft

multiple PSOs are applied to a user or group object. A low value for the msDS-PasswordSettings Precedence attribute indicates that the PSO has a higher priority than other PSOs. For example, imagine that a user object has two PSOs linked to it: one PSO that has an msDS-PasswordSettings Precedence value of 10 and another PSO that has a value of 40. In this case, the PSO that has the msDS-PasswordSettingsPrecedence value of 10 (the lower value) has a higher rank and will be applied to the user object. If multiple PSOs are linked to a user or group, the logic that Server 2008 uses to determine the resultant PSO is as follows:

- A PSO that is linked directly to the user object is the resultant PSO. If more than one PSO is linked directly to the user object, the PSO with the lowest msDS-PasswordSettingsPrecedence value is the resultant PSO.
- If no PSO is linked to the user object, but PSOs are linked to global groups the user is a member of, Server 2008 compares the msDS-PasswordSettingsPrecedence values of these different global group PSOs. Again, the PSO with the lowest msDS-PasswordSettingsPrecedence value is the resultant PSO.
- If no PSO is obtained from these conditions, the "classic" Default Domain Policy is applied.

To let administrators easily determine the PSO that's ultimately applied to a user, Microsoft added a new attribute called msDS-ResultantPSO to each AD user object. This attribute holds the distinguished name (DN) of the PSO that's applied to a given user.

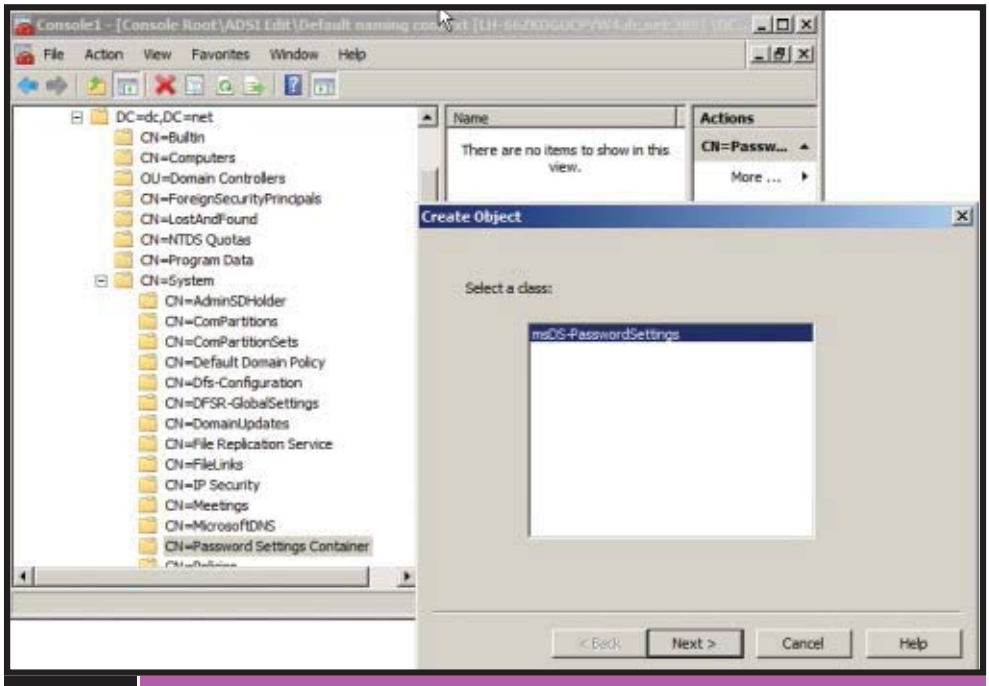


Figure 1: Using ADSI Edit to create a PSO

PSO Creation and Configuration Tools

Microsoft doesn't plan to provide a GUI tool or Microsoft Management Console (MMC) snap-in extension to configure fine-grained password policies in the first Server 2008 release. However, you can use existing LDAP query tools such as LDP or LDIFDE, or the MMC ADSI Edit snap-in, to define and configure PSOs. These tools are available on any Server 2008 AD installation. Although these three tools are rather complex, experienced AD administrators should have no problem using them to set the new password policies.

Novice AD administrators, or experienced administrators who simply want to make their jobs easier, might consider Joe Richards' command-line tool called psomgr.exe, or Special Operations Software's Specops Password Policy tool. Specops Password Policy lets you use a special MMC snap-in to configure PSOs from the Windows GUI. Both tools hide the AD complexity behind fine-grained password policies and significantly ease their configuration. You can download the PSOMgr tool from www.joeware.net/freetools/tools/psomgr. The full-featured commercial version of Specops Password Policy is available at www.specopssoft.com/products/specopspasswordpolicy; a free version with limited functionality, called Specops Password Policy Basic, is available at www.specopssoft.com/wiki/index.php/specopspasswordpolicybasic. The full-featured version extends the standard Windows password policy capabilities by adding features such as the ability to disallow the use of user names or certain words in passwords, and automatic user notification of password expiry via email message.

To use ADSI Edit to define a new PSO, start ADSI Edit and connect to the domain where you want to define a fine-grained password policy. Then, navigate to the System\Password Policy Settings container. Right-click the container and select New, Object. In the Create Object dialog box, which Figure 1 shows, select the msDS-PasswordSettings object class, and enter your preferred password and account lockout policy values for the different PSO attributes.

To use LDP to define a new PSO, you must initiate several LDAP commands from the LDP interface. (For information about using LDP, see the Microsoft article "Using Ldp.exe to Find Data in the Active Directory," at support.microsoft.com/kb/224543.) To use the LDIFDE command line to define a new PSO, you must first create an LDF configuration file that specifies the different PSO attributes. (For information about using LDIFDE, see the Microsoft article "Using LDIFDE to import and export directory objects to Active Directory," at support.microsoft.com/kb/237677. For more detailed instructions, see the Microsoft article "Step-by-Step Guide for Fine-Grained Password and Account Lockout Policy Configuration," at technet2.microsoft.com/windowsserver2008/en/library/2199dcf7-68fd-4315-87cc-ade35f8978ea1033.mspx?mfr=true.)

When you use the ADSI Edit version that's bundled with Server 2008 to define PSOs, you must enter the four time-related PSO attributes (msDS-MaximumPasswordAge, msDS-MinimumPasswordAge, msDS-LockoutObserva-

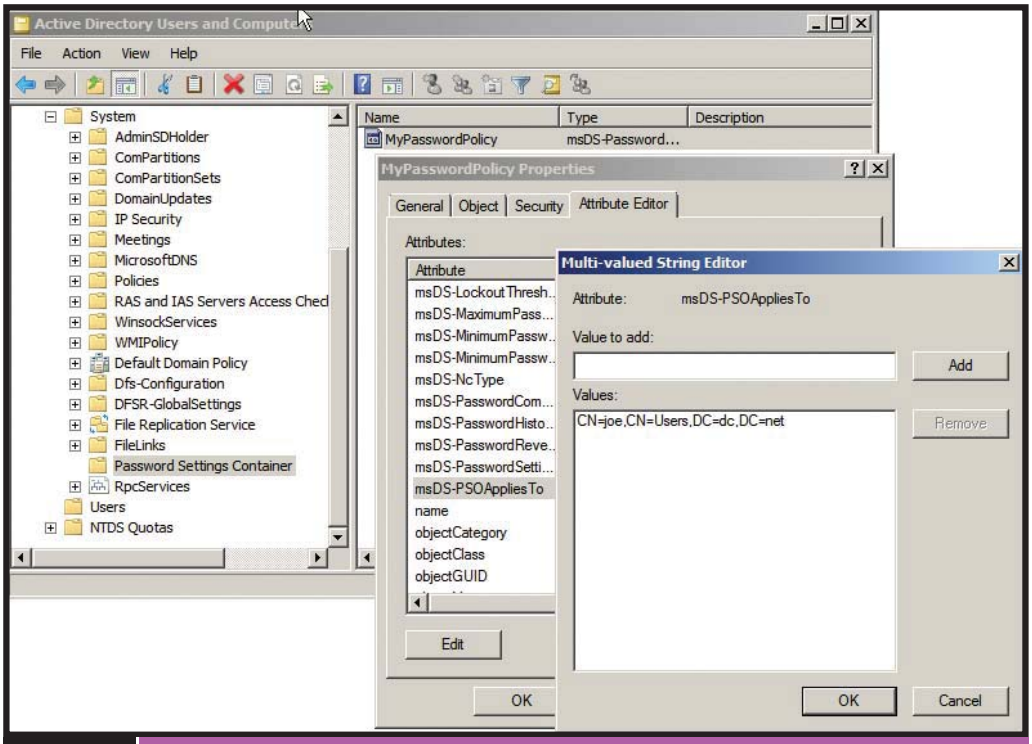


Figure 2: Modifying the user objects a PSO is linked to from the MMC Active Directory Users and Computers snap-in

tionWindow, and msDS-LockoutDuration) in the days:hours:minutes:seconds format. For example, to set a maximum password age of 40 days, you'd enter the value 40:00:00:00.

When you use the ldifde command or an older (pre-Server 2008) version of ADSI Edit to create PSOs, you must enter the values of these attributes in I8 format (i.e., integer represented in 8 bytes). In the I8 format, time must be stored in intervals of -100 nanoseconds. This means that to use LDIFDE or an older ADSI Edit version to set PSO attributes to their appropriate values, you must convert the time you want to set in values in minutes, hours, or days to time values in intervals of 100 nanoseconds, then precede the resultant values with a minus sign (-).

Because the I8 format is difficult to use, I recommend that you use the Server 2008 version of the ADSI Edit tool (or the PSOMgr or Specops Password Policy tools) for defining PSOs. The Microsoft article "Step-by-Step Guide for Fine-Grained Password and Account Lockout Policy Configuration" (technet2.microsoft.com/windowsserver2008/en/library/2199dcf7-68fd-4315-87cc-ade35f8978ea1033.mspx?mfr=true) explains I8 conversion in more detail.

In addition to using ADSI Edit, LDP, LDIFDE, PSOMgr, or Specops Password Policy to link PSOs to users or global groups, you can also use the MMC Active Directory Users and Computers snap-in. To link a PSO to a user or group from this snap-in, open the snap-in and ensure that the Advanced Features view is enabled. (To enable this view, use the Advanced Features option in the View menu.) Then, open the Passwords Settings Container in the System container, right-click the PSO you want to link, and select Properties. In the Properties dialog box, select the Attribute Editor tab, select the msDS-PSOAppliesTo attribute, and click Edit. Finally, in the Edit dialog box, which Figure 2 shows, enter the DN of the user or group you want to link the PSO to. If you don't know the correct DN of a user or group, you can obtain it from the Active Directory Users and Computers snap-in. In the snap-in's details pane, right-click the user or the global security group, select Properties, select the Attribute Editor tab, and view the value of the user's or group's distinguishedName attribute in the Attributes list.

A Valuable Addition

Server 2008's fine-grained password and account lockout policies are a valuable addition to the Windows security management portfolio. Although defining and configuring these policies isn't straightforward in the first Server 2008 release (I strongly advise you to use PSOMgr or the Specops Password Policy tool), the policies do provide a significant level of additional flexibility. For example, Server 2008's fine-grained password policies eliminate the need for organizations to define additional Windows domains or develop special password filters.

InstantDoc ID 97567

Leveraging Server 2008's Password Policies

Step 1 Windows Server 2003 and Windows 2000 Server password policies let administrators define only one password policy that applies to all user accounts in a domain.

Step 2 Windows Server 2008 introduces fine-grained password policies that let administrators define different password policies for different domain account categories in a single domain.

Step 3 Create Password Settings objects (PSOs) to define new fine-grained password policies.

Step 4 To define and configure the PSOs you created, use an LDAP query tool (e.g., LDP, LDIFDE, ADSI Edit), the PSOMgr or Specops Password Policy tools, or the MMC Active Directory Users and Computers snap-in.

InstantDoc ID 97741

Introducing an integrated approach to complete SharePoint protection and management

DocAve™ Software for SharePoint

Changing the way Administrators manage SharePoint

FREE 30 DAY TRIAL
Download at
www.avepoint.com

SharePoint management made simple.

Now you can control and manage the back-end of all your SharePoint environments from one place. DocAve is the only truly integrated, easy-to-use software that offers a complete set of SharePoint backup, recovery, and administration tools. One solution, with many mix-and-match functions, now gives you power like never before.

Complete SharePoint protection.

With item-level backup and full-fidelity restore, DocAve allows for fast recovery of business critical documents and content. Complete SharePoint platform backup allows for quick and painless recovery of the entire system during a disaster. With DocAve, you'll have complete confidence in your SharePoint environment.

AvePoint

Call 1-800-661-6588 or visit www.AvePoint.com for more information or to download a free trial.

Office & SharePoint PRO

officesharepointpro.com

Using Content Types in Windows SharePoint Services 3.0

Categorize and organize your SharePoint libraries and lists

by Douglas Ryan VanBenthuysen

One of the concepts at the core of Windows SharePoint Services (WSS) 3.0 is the improvement to document storage called content types. In WSS 2.0, each list (whether a document library or a regular SharePoint list) was bound to a single schema, and the schema resided within that list. With the content type innovation, a list can contain multiple schemas, and a schema can be used in multiple lists. The schema for a content type can include metadata (which would appear as columns in a SharePoint list), document templates, workflows, the document information panel, and other customizations. What this all means is that you can store the same type of content in more than one list and store more than one type of content in the same list, thus eliminating the need for multiple libraries containing information that you'd like stored in the same place. In this article, I walk you through the process of creating and customizing a content type and associating it with a document library to achieve the benefits of this useful innovation.

A Sample Library with Multiple Content Types

Let's begin by taking a look at a document library that contains multiple content types. In the example that Figure 1 shows, a company's sales team maintains a document library for various types of sales documents, including sales presentations, financial analyses, and RFP responses. The most obvious effect of content types on this library is the ability to choose different templates for the different types of documents. Thus, when you click the arrow beside New, you get a choice of the available content types.

Notice that the various content types in this library have different columns of metadata. For example, the column Deal Size contains only data for the Financial Analysis content type. Also note that all of the content types contain information in the Client column.

The template and metadata columns are two key parts of the schema for a content type. In earlier versions of SharePoint, assigning different templates and metadata columns would have required the creation of multiple document libraries. Now, let's look at the process of creating content types.

Creating a New Content Type

When creating a content type, you first need to decide whether you want to create it on the root site level, the child site level, or the list level. Essentially, if you create the content type on one of the site levels, it will be available for all child sites and lists in that site collection; if you create it on the list level, it will be available for that list only. For example, the document

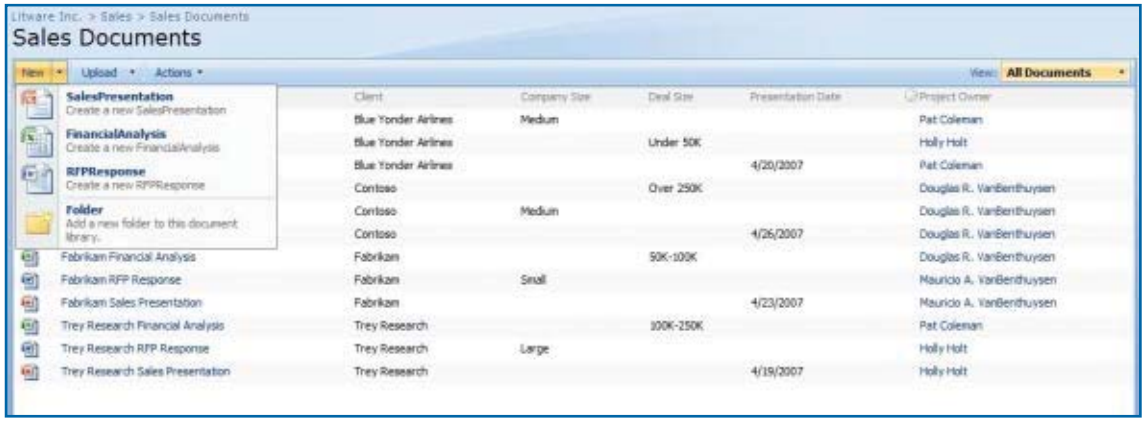


Figure 1: *A WSS 3.0 document library containing three content types*

Learning Path

WINDOWS IT PRO RESOURCES

Learning about SharePoint:

"SharePoint Server 2007 Revealed," InstantDoc ID 94914

"Windows SharePoint Services 3.0 Out of the Box," InstantDoc ID 94240

"The File Share Is Dead: Long Live SharePoint Document Libraries," InstantDoc ID 95480

MICROSOFT RESOURCES

Microsoft Windows SharePoint Services 3.0
office.microsoft.com/en-us/sharepointtechnology/FX100503841033.aspx

Welcome to the Microsoft Office SharePoint Server 2007 SDK
msdn2.microsoft.com/en-us/library/ms550992.aspx

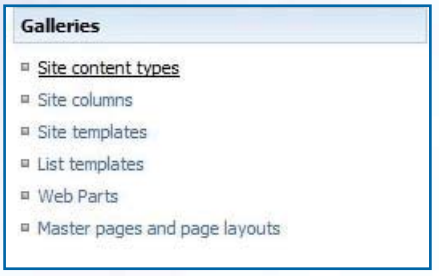


Figure 2: *Galleries available in Site Settings*

Figure 3: *Content type creation form*

document library that Figure 1 shows resides at moss.litwareinc.com/SalesNew/SalesDocument; that is the Sales Document library in the new sales site, which is a child of the Litwareinc site. When creating a new content type that can be used in this document library, you can either create it at the Litwareinc (root site) level, at the New Sales (child site) level, or the Sales Documents (list) level. As a general rule, I find it best to create content types at the highest level possible because the content type will then be available to as much of the site as possible. There are, however, several reasons you might want to create a content type at an individual site or list level. For example:

- You want to restrict use of a content type to a particular list.
- Your content type needs to incorporate columns created at the list level.
- You lack permission to create the content type at a higher level.
- When creating a child content type based on an existing content type, you might want to have the parent on the site level but the child on the list level.

I'll show you how to create a content type at the root site level, but the steps are basically the same for creating content types at the child site or list level. To create a content type, select Site Actions, Site Settings, Modify All Site Settings. This choice will bring up various settings, including the list of galleries, which contains an option called *Site content types*, as Figure 2 shows. Click *Site content types* to display the available content types. Select the option to create a new content type, which opens the content type creation form that Figure 3 shows.

I've chosen to create a content type for writing letters because you might want to use such a content type throughout your organization, and using content types will let you use a company letter template, with consistent letterhead and formatting.

The Parent Content Type choices affect what settings will apply to the content type. For our letter content type, we'll base the content type on one of the basic out-of-the-box content types. Choosing the Document parent content type will result in the content type having a blank Microsoft Office Word document for its template, minimal metadata columns, and no further customizations. You can also choose to place your new content type in an existing or custom group. Placing the content type in a group makes it easier to find when you want to work with it later.

Customizing a Content Type

Now that we've created our content type, we want to customize its schema to maximize our benefit. The screen that Web Figure 1, at www.windowsitpro.com, InstantDoc ID 97483, shows will appear after you create the content type. You can also access this screen through the site content types gallery or by clicking the content type in Document Library Settings after you've associated the content type with a list. On this screen you can select or change the following settings:

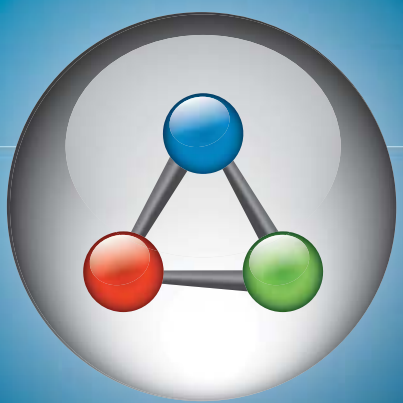
- *Name, description, and group.* These options let you change the settings you chose when creating the content type.
- *Advanced settings.* These primarily let you choose a template. You can choose as a template any document to which you can browse, whether it resides on your site or locally. Note also that you don't need to select a template file (such as a .dotx file for Word).
- *Workflow settings.* These let you select a workflow to be associated with a content type. This option is one of the most compelling parts of using content types because it lets you have different workflows for different content types within the same document library and lets you reuse the workflow setting on additional document libraries without the need for reconfiguration. When you select Workflow settings, you'll be able to choose from the out-of-the-box workflows or any custom Visual Studio workflows. Currently, you can't associate SharePoint Designer workflows with a content type. Let's hope this functionality is coming. After you associate a content type with a list, however, a SharePoint Designer workflow can be developed and attached to the list.
- *Document information panel settings.* These let you upload or modify the document information panel that documents created with the content type use. As you can see in Figure 4, page 62, the document information panel is an Office InfoPath form that serves as a properties pane for documents that open from SharePoint. It links metadata columns to the document, and you can drive a lot of the business logic in your Word document with the declarative rules engine of InfoPath, without having to write any

I find it best to create content types at the highest level possible because the content type will then be available to as much of the site as possible.

busi·ness
pro·cess
au·to·ma·tion

[biz-nis | pros-es | aw-tuh-mey-shuhn]

The replacement of a manual business process with an automated one, usually through the use of **advanced technologies**.



AutoMate BPA Server 7™

The Business Process Automation Server from Network Automation

NO CODE, NO LIMITS

Automates business & IT processes
Eliminates the need for job schedulers, scripts & batch files
Intuitive drag-and-drop workflow design & task development

Visit **WhatIsBPAServer.com** to learn more about **BPA Server 7** and how the world leader in **Business Process Automation** is advancing the field. Again.

NETWORK AUTOMATION

www.WhatIsBPAServer.com
888-786-4796

Redmond MVP Most Valuable Product

Windows IT Pro READERS CHOICE 2006 Winner

Windows IT Pro EDITOR'S BEST 2007 WINNER

code. On this form, you can upload a custom information panel (an XSN, or InfoPath form template file) and choose whether you want the information panel to always open by default.

- *Information management policy settings* let you define or associate custom policy settings with the content type.
- *Manage document conversion for this content type settings.* Choosing this option requires that document conversion be enabled for your site collection. (An administrator must enable document conversion in Central Administration.)

Adding Columns

Adding columns to the content type defines the metadata that will be available for SharePoint lists and the document information panel. Creating a column is similar to creating a content type and can be done at either the site level or the list level.

For our letter content type, we'll add an existing column and create a few new columns. To add the existing column, simply click *Add from existing site columns* on the Site Content Types page. You'll then see a list of all available columns that you can add to the content type. To create a new site column, click *Add from new site column*. This selection will bring up the New Site Column creation form, which Web Figure 2 shows. On this form, you can enter the Column name (e.g., Letter Date) and the type of information (e.g., Date and Time). The data type you select determines the other options that will be presented. After you've customized the content type, you're ready to associate it with a document library.

Associating a Content Type with a SharePoint Document Library

Because we created the content type on the site level, we have to associate it with a list. Thinking back to the Sales Document Library we looked at earlier, the sales team has decided to start storing sales letters in the same library. This decision will help keep things organized: Sales team members can easily sort the library to group letters and other contract information without having to create multiple folders.

When you go to the document library settings, because content types have already been enabled for this document library (you'll see how to enable content types for a document library in the Reusing a Content Type section later in this article), you'll see a section called Content Types, which shows the content types currently available in the document library, as well as the option to add a new content type. When you choose to select a new content type, you'll see a form that lets you select from available content types, as Web Figure 3 shows. Select the desired content type (e.g., Letter) and click Add. The new content type will now be available as a selection in the document library.

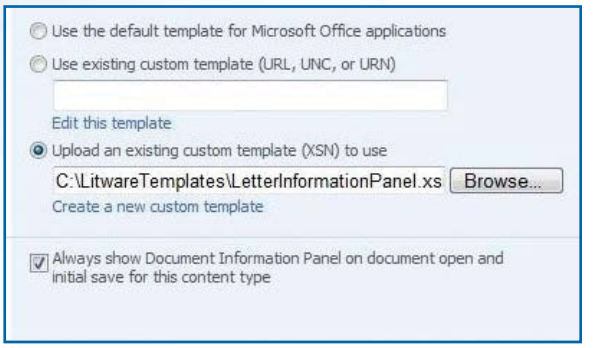


Figure 4: *Selecting a Document Information Panel template*

Now, when you open a new document based on the content type, it will open with the designated template and document information panel, as Figure 5 shows. Notice that the document contains the company letterhead and a basic letter format with content controls (e.g., the Client content control that Figure 5 shows). These content controls are linked to the document information panel. So, if you were to add the client's name in the document, it would update in the document information panel. If you were to change the date in the information panel, it would update in the document. Additionally, this data will be available in the SharePoint list.

When you save the document back to the library, the custom metadata columns for this content type appear in the document library, as Figure 6 shows. (I had to adjust the default view to get the columns to appear. The columns are available to the document library as soon as you add the content type, but they must be selected in the settings page for the view.) Note that in this example, we chose to add the Letter site content type directly to this list. You also could

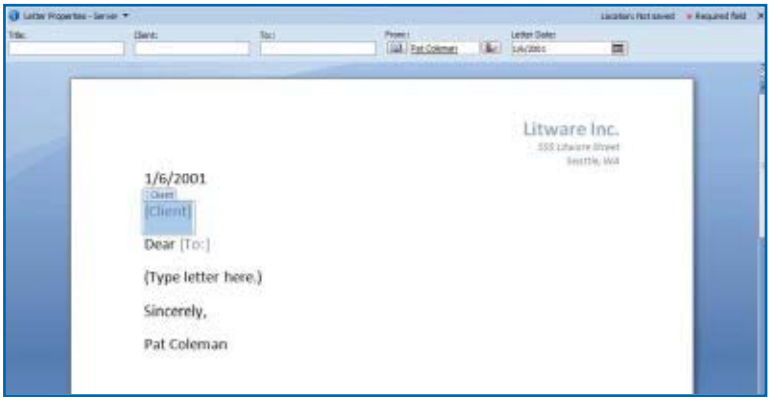


Figure 5: *New document based on the new content type*

Figure 6: *Document library with new content type*

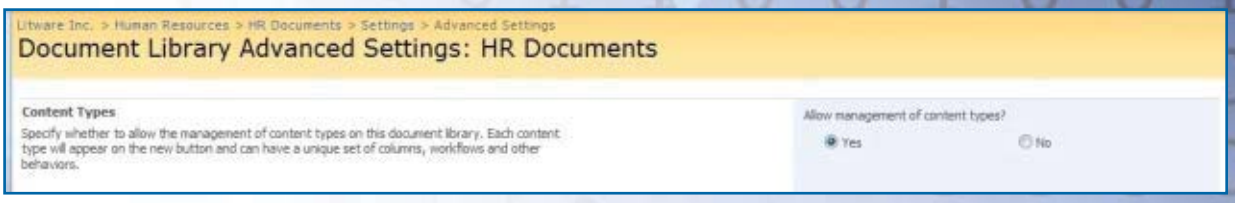


Figure 7: *Enabling content types for a document library*

have created a child content type based on the Letter content type, which would be useful if you want to use the same template throughout the organization but want different workflow settings for different departments.

Reusing a Content Type

Reusing a content type is as simple as associating it with another document library. For example, you could create a new site for your human resources department, with a document library called HR Documents. Because this is a new library, you must first enable management of content types for the library, which you do by opening the Document Library Advanced Settings, and selecting *Allow management of content types,* as Figure 7 shows.

After content types are enabled, you can add the Letter content type using the procedure described earlier. Again, you might choose to create a child content type called HR Letter at the list level. The advantage of using child content types like this is that if the parent is updated, all the children can be updated as well. For example, if HR Letter and Sales Letter are both children of Letter, and you want to change the letterhead, you only need to update the template for the Letter content type; the template for HR Letter and Sales Letter will be inherited from the parent.

Reaping the Benefits

Content types define schema for objects stored in WSS 3.0, allowing you to both store the same type of content in more than one list and to store more than one type of content in the same list. By using content types, you save yourself from having to create multiple document libraries to store data that might be better off stored in the same place. With the ease of sorting information in SharePoint, you're much better off with a library full of many types of documents than with a whole bunch of libraries. Additionally, content types save you from having to create settings several times if you want to use the same type of document in multiple locations.

InstantDoc ID 97483

Douglas Ryan VanBenthuysen (doug@wordswordswords.us) is pursuing his Ph.D. in Old English Literature at the University of New Mexico. He was formerly a solutions specialist for 3Sharp, a technical services company that focuses on Microsoft technology solutions.

Q: How do I enable an additional SMTP address for a Microsoft Exchange Server organization?

A: You use recipient policies to control email address-generation for an Exchange organization. To add a new SMTP address, perform these steps:

1. Start Exchange System Manager (ESM).
2. Expand the Recipients container in the navigation pane and select Recipient Policies.
3. Right-click Default Policy in the details pane and select Properties.
4. Select the E-Mail Addresses (Policy) tab.
5. Click New.
6. Select the address type (e.g., SMTP Address) from the displayed dialog box and click OK.
7. Enter the new address. The default format for entering the address is

```
user_name@domain_name.com
```

but you can use control characters to control how the unique part of the name (i.e., user_name) will be generated, as Figure 1 shows. These are the control characters you can use:

- %s–surname (last name)
- %g–given name (first name)
- %I–middle initial
- %d–display name
- %m–Exchange 2003 alias
- %rxy–Replace all subsequent characters x with character y in username. If x = y, the character will be deleted.

Additionally if you add a number between the % and the character, it will use that number of characters (e.g., %1g will use only the initial of the first name).

8. Click OK.

Select the checkbox next to the new address to enable it and ensure it's generated for all users. If you want the new SMTP address to be the primary address, select the new entry and click *Set as Primary*.

InstantDoc ID 97546

—John Savill

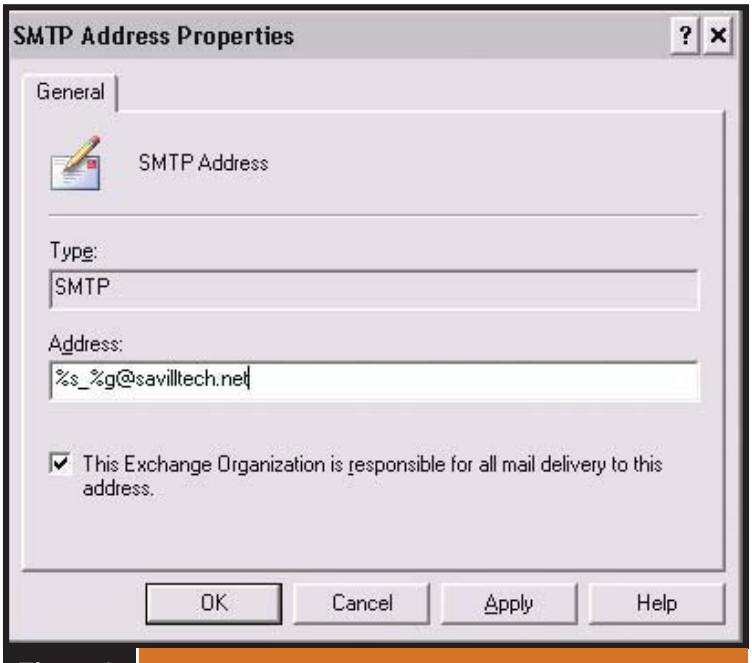


Figure 1: Using control characters to generate email addresses

Q: How do I manage POP3 and IMAP4 services in Microsoft Exchange Server 2007?

A: The Exchange 2007 UI doesn't support POP3 and IMAP4 management. Microsoft plans to add this support to the interface as part of Exchange 2007 SP1. You use the Exchange Management Shell Set-PopSettings and Set-ImapSettings cmdlets to manage POP3 and IMAP4. To learn more about managing POP3 and IMAP4, see the article "Managing POP3 and IMAP4" at technet.microsoft.com/en-us/library/l4478379-227e-43f0-82le-3d0f3a6c259c.aspx.

InstantDoc ID 97545

—John Savill

At a Glance

Q: How can I configure where Windows Deployment Services creates computer objects?

A: By default, Windows Deployment Services creates computer objects in the default Computers container for the domain. However, you can configure Windows Deployment Services to create objects in

Mark Russinovich (mark.russinovich@microsoft.com)

John Savill (jsavill@windowsitpro.com)

Ask the Windows IT Pro Community

For answers to more of your Windows server and client systems questions, visit our online discussion forums at www.windowsitpro.com/forums.

an alternate location by using the Wdsutil command with the /NewMachineOU switch. The command gives you several configuration options, including the option to create the computer object in the Windows Deployment Services domain, in the user's domain, in the same organizational unit (OU) as the user, or in a custom OU location. For example, to create computer objects in a custom OU (e.g., AutoComp in the savilltech.net domain), you would use the following command:

```
C:\Users\Administrator.
SAVILLTECH>wdsutil /set-
server /newmachineou /type:
custom /ou:ou=AutoComp,dc=sav
illtech,dc=net
```

InstantDoc ID 97547

—John Savill

Q: How do I set my system path to include, by default, the core Windows Automated Installation Kit (AIK) utilities (e.g., ImageX?).

A: To enable the core Windows AIK commands to be accessible from your environment, you need to add the following paths to your system path:
C:\Program Files\Windows AIK\Tools\PETools\
C:\Program Files\Windows AIK\Tools\<architecture> (e.g., AMD64)

To add the paths, open the System Control Panel applet, select the Advanced tab, and click Environment Variables. Under the System variables section, select Path, click Edit, and add the above paths, separated by a semicolon.

InstantDoc ID 97351

—John Savill

The Case of the Failed File Copy

This is a summary of a popular posting to Mark Russinovich's technical blog (https://blogs.technet.com/markrussinovich/about.aspx), which covers topics such as Windows troubleshooting, technologies, and security. You can read the entire post at https://blogs.technet.com/markrussinovich/archive/2007/10/01/2087460.aspx

The other day a friend of mine called to tell me that he was having a problem copying pictures to a USB flash drive. He'd been able to copy more than two hundred files when he got the error message *The directory or file cannot be created,* after which he couldn't copy any more files without getting the same message.

Unfortunately, the message provides no clue as to the underlying cause, and the dialog box explains that the error is unexpected and doesn't suggest where you can find the "additional help" to which it refers. My friend was sophisticated enough to make sure the drive had plenty of free space, and he ran Chkdsk to check for corruption, but the scan didn't find any problem. The error persisted on subsequent attempts to copy more files to the drive. At a loss, he turned to me.

I asked him to capture a trace with Process Monitor, a real-time file system and registry monitoring tool, which would reveal actual OS errors returned by the file system. He sent me the resulting Process Monitor PML file, which I opened on my own system. After setting a filter for the volume in question to narrow the output to just the operations related to the file copy, I went to the end of the trace to look back for errors. I didn't have to look far; the last line appeared to be the operation causing the error.

I'd never seen or even heard of the error message "STATUS_CANNOT_MAKE." At that point, I could have cheated and searched the Windows source code for the error, but I decided to see how someone without source access would troubleshoot the problem. A Web search took me to an old thread in a newsgroup for Windows file system developers. It told me that the problem might be that if you try to create a file in the root directory of a FAT12 system, there might not be enough available directory entries.

Sure enough, the volume was formatted with the FAT file system and the number of files on the drive, including those with long file names, could certainly have accounted for the use of all available 512 root-directory entries.

I had solved the mystery. I told my friend he had two options: He could create a subdirectory off the volume's root, and copy the remaining files into it, or he could reformat the volume with the FAT32 file system, which removes the limitation on entries in the root directory.

One question remained, however. Why was the volume formatted as FAT instead of FAT32? The answer lies with both the USB drive makers and Windows format dialog. I'm not sure what convention the makers follow, but my guess is that many format their drives with FAT simply because it's the file system guaranteed to work on virtually any OS, including those that don't support FAT32, such as DOS 6.0 and Windows 95.

As for Windows, I would have expected it to always default to FAT32, but a quick look at the Format dialog box's pick for one of my USB drives showed that I was wrong. After some research, I found that Windows defaults to FAT for non-CD-ROM removable volumes that are smaller than 4GB in size.

I'd consider this case closed, but I have two loose ends to follow up: See if I can get the error message fixed so that it's more descriptive, and lobby to get the default format changed to FAT32. Wish me luck.

—Mark Russinovich

InstantDoc ID 97352

Protect Your Data with Cipher

Wield EFS power over your folders, subfolders, and files

Ever since the debut of Windows 2000 Server, you've had a built-in way to protect files on your systems—Encrypting File System (EFS). The Win2K edition of EFS suffers from a few glaring security holes, but the Windows Vista and Windows XP versions are much more effective. In fact, EFS is extremely secure on a Vista box running BitLocker.

The GUIs of Vista and XP offer some access to EFS's power, but to really see EFS's payoff, you need to dig into EFS's command-line interface, which is a program called Cipher. (For the purpose of this article, I'll use the Vista version of Cipher, but XP's Cipher is similar.) Without further ado, let's dive into the workings of this encryption/decryption tool.

Encrypting and Decrypting

Cipher provides effective encryption and decryption functionality through its /e (encrypt) and /d (decrypt) options. To use Cipher in this way, simply follow the /e or /d option with the name of a file or folder you want to encrypt or decrypt. For example, you would use Cipher /e secret.txt to encrypt the single file secret.txt, Cipher /e secret*.txt to encrypt every file that matches that pattern, and Cipher /e C:\mysecrets to encrypt everything in the C:\mysecrets folder.

By default, however, instructing Cipher to encrypt a folder doesn't cause the tool to encrypt files already in the folder; instead, it causes Windows to encrypt any *new* files in the folder. Thus, to encrypt C:\mysecrets *and* ensure that any files already in C:\mysecrets are encrypted, you would type two commands:

```
cipher /e C:\mysecrets
cipher /e C:\mysecrets\*
```

After you encrypt the folder, you'll be able to read a file but other users won't. This user-transparency is one of EFS's greatest strengths.

What if you want Cipher to not only encrypt a folder and any new contents but to encrypt the folder, its subfolders, and files in that folder and subfolders? You would use the /s: option to specify the top-level folder. For example, to encrypt C:\mysecrets, its folders, and its subfolders, you would type

```
cipher /e /s:C:\mysecrets
```

That's not a misprint: To work on subfolders and files, you don't just name the top-level folder. You prefix the folder's name with the /s: option, and you leave no space between the option and the folder name.

In practice, it's always a good idea to encrypt folders, and it's almost never a good idea to encrypt particular files. When EFS encrypts a file, it works from a temporary file that contains the unencrypted version of the file's contents. It then deletes the file, but it doesn't take the time to wipe the temporary file's clusters clean. Therefore, it's theoretically possible that someone could discover an encrypted file's contents by digging up the remnants of EFS's temporary file. The result of encrypting *inside* a folder is that those temporary files reside inside the folder and are therefore not susceptible to prying eyes. Probably for that reason, the Windows Server 2003 and XP version of Cipher works only on folders and ignores any file references, unless you add the /a option. (Vista's version doesn't seem to need the /a option.) Thus, Cipher /e secret.txt would have no effect on Windows 2003 or XP, but Cipher /e secret.txt /a would encrypt secret.txt.

The /d option works as /e does, but in reverse. Cipher /d C:\mysecrets would instruct Windows to not encrypt any newly created files in C:\mysecrets. You'd have to use Cipher /d C:\mysecrets* to decrypt any currently encrypted files in C:\mysecrets.

Mark Minasi (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books, including *Administering Windows Vista Security: The Big Surprises* (Sybex). He writes and speaks around the world about Windows networking.

To really see EFS's payoff, you need to dig into EFS's command-line interface.

Adding the /h option instructs Cipher to display the names of any hidden or system files that it has worked on. By default, Cipher encrypts or decrypts any files in a given folder, but it doesn't report on them. Adding the /b option instructs Vista's Cipher to stop if it runs into any errors. (By default, the tool continues encrypting or decrypting in spite of any errors it encounters.) For the Windows 2003 or XP version of Cipher, you use the /i option to do the same thing.

Valuable Tool

The ability to encrypt and decrypt files from the command line can be useful when you're working with a low-bandwidth remote-control tool such as XP's Telnet or Vista's Winrs command. It's also valuable when you want to automate the process of placing folders onto systems and simultaneously securing them. But Cipher does a lot more, as I'll demonstrate next month.

InstantDoc ID 97506

Windows Vista Annoyances

Software and hardware incompatibilities, lost settings, and the dreaded UAC give users plenty to grumble about

You've heard the hype: Windows Vista is the new desktop standard! Vista has sold 40 million copies! Vista is Microsoft's best desktop OS ever! But you look around and no one in your office is using it, so you become the official Vista guinea pig. Soon, you discover a host of Vista annoyances to scare (or share with) your coworkers. Here are my top 10 Vista annoyances.

10 **Application incompatibility**—Without a doubt, application incompatibility is Vista's Achilles' heel, particularly in upgrade scenarios. In a business environment, Vista was OK running applications such as Office. But my home upgrade was a nightmare. Nero and Roxio products were the first to throw up their hands. Many of my games were close behind, often hamstrung with User Account Control (UAC) messages. Most companies have updates available, but you usually need to upgrade to the next release to get Vista compatibility.

9 **Windows Aero hardware requirements**—Superficially, the most compelling reason to migrate from Windows XP to Vista is the Aero interface. Unfortunately, Aero requires modern graphic capabilities such as a minimum of 128MB of video RAM, and it doesn't work on most older systems that use an integrated video adapter. Some older systems support an add-on video graphics adapter, but many don't.

8 **Too much UAC**—Although I understand the concept behind UAC, the fact is it's never prompted me for anything meaningful; it simply adds more dialog boxes to common administrative tasks. I keep it turned on in case it ever stops something important, but you can disable UAC in the User Accounts Control Panel applet.

7 **Lost wallpapers and themes**—After upgrading to Vista, all my themes and desktop wallpapers were replaced by new and, to me, unattractive substitutes. And, while Microsoft was changing everything else, why didn't they move the power options out of the Screen Saver tab to their own tab?

6 **Losing Windows Explorer settings**—On the subject of losing things, why can't Vista's Windows Explorer remember settings for different folders? Try as I might, I can't make it maintain the sort order I prefer. It stays for a while, but it always returns to the alphabetical file listing eventually.

5 **Explorer drag-and-drop**—Another really annoying feature in Vista's Windows Explorer is that it drops files where your cursor is. When I have folders organized by date and I drop a new file into a folder, I want it to go to the bottom as the newest item. Vista places it wherever in the list you release the mouse.

4 **Antivirus incompatibility**—Like the application software incompatibility problem, the answer to antivirus incompatibility is to purchase an upgrade to a Vista-compatible release. If you want to run the Vista x64 version, you might need to switch products because not all antivirus vendors support the x64 edition.

3 **VMware virtualization software**—My copy of VMware Workstation 5.5 has always refused to run under Vista. Rather than buy the new version of Workstation, I switched to VMware Server 1.03. However, I ran into a driver problem where, for some inexplicable reason, VMware doesn't sign their drivers. To get VMware Server to work on Vista, press F8 when the system boots and select Disable Driver Signature Enforcement.

2 **Dual-boot difficulties**—On XP, virtualization nearly eliminated my desire to create dual-boot systems. But Vista's incompatibilities with my favorite VMware products combined with a pressing need to test various scenarios quickly brought back the idea of dual-booting. Unfortunately, the good old boot.ini is gone and XP's simple boot process has been replaced with Vista's nearly inscrutable Boot Configuration Data Editor (bcdedit.exe). I've created several Vista dual-boot systems, but it's not nearly as easy as it was under XP.

1 **All-in-Wonder incompatibility**—This is my biggest pet peeve with Vista. This might be a more generic driver incompatibility problem, but the ATI All-in-Wonder card is where I ran into it. ATI's supposedly Vista-compatible cards don't provide video capture support like they did under XP. What's worse is that this product has a "Works with Windows Vista" logo even though it doesn't provide full functionality. That's just wrong.

InstantDoc ID 97490

Michael Otey (mikeo@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and coauthor of *SQL Server 2005 Developer's Guide* (Osborne/McGraw-Hill).

Jeff James (jjames@windowsitpro.com)
is senior editor, products, for *Windows IT Pro* and *SQL Server Magazine*.

At a Glance

Readers Review HOT PRODUCTS

Manage and Track Code Changes

SourceAnywhere Standalone

I'm a developer, and I've been writing code since 1979. I've never been a project manager (I usually hire one) and prefer to write code myself. I had been using Microsoft Visual Source Safe (VSS) for some time, but VSS began driving me crazy. At one point, we were a team of eight using VSS all day, every day, to help us convert between Microsoft Visual FoxPro and VB.NET. VSS was corrupting its "database" weekly—and I truly object to calling files in a directory structure a database—and I was spending too much time rebuilding it. I had to spend hours every week fighting with VSS, and often had to rebuild it from scratch. I began looking for a better solution and did an Internet search for "source code control." **SourceAnywhere Standalone** (SAS) came up, so I gave it a try. That was sometime in January 2005, and I've been using SAS every since.

Reader: Les Pinter, Founder, Pinter Consulting
Product: SourceAnywhere Standalone
Company: Dynamsoft
Contact: Dynamsoft.com

Installation was straightforward: I followed the installation instructions, and it worked the first time. I've always felt that a source code manager needs to be unobtrusive and practically transparent, to the point that the user doesn't even know it's there, and I feel that way about SAS. It doesn't get between me and the primary job, which is making code work. SAS is faster than a bandit, the interface is intuitive and easy to understand, and it doesn't break. I also like the idea of using SQL Server to store repository data—it's what a database is for. This is the source code management tool I was looking for.

"SourceAnywhere Standalone is faster than a bandit, the interface is intuitive and easy to understand, and it doesn't break."

—Les Pinter, founder, Pinter Consulting

What's Hot continues on page 71

Wanted: Your Real-World Experiences with Products
Have you discovered a great product that saves you time and money? Do you use something you wouldn't wish on anyone? Tell the world in a review right here in What's Hot: Readers Review Hot Products. If we publish your opinion, we'll send you a Best Buy gift card! Send information about a product you use and whether it helps you or hinders you to whatshot@windowsitpro.com.

Manage and Secure Unstructured Data

Varonis Data Governance

Reader:
Chuck Klawans
Information Security Officer
Product:
Varonis Data Governance
Company:
Varonis
Contact:
www.varonis.com

I work as the information security officer for the Children's Hospital of Wisconsin, and I was looking for a software solution to help maintain compliance with the Health Insurance Portability and Accountability Act (HIPAA), which regulates our use of patient information. Because we have patient information on Windows file servers, we not only have to ensure that only the appropriate people have access to the information but also have an audit trail of access to the information. Turning on file-level auditing on Windows servers isn't an option (due to the resources that would be consumed), so I needed an alternative solution. I also needed a way to view user and group permissions across resources, in a concise format.

A VAR that the hospital works with brought **Varonis Data Governance** to my attention. I've worked closely with this partner, who understands the hospital's needs and regulatory requirements, so the VAR was sure I would be interested. After choosing to go with Varonis, I found the installation to be very easy. I worked with Varonis before the implementation to make sure that the hospital's server and SQL setups met the system requirements. Because everything was in place, installing the system engine and client software took less than an hour.

Some of my favorite features include the ability to record all access to unstructured Windows resources in an efficient manner. The hospital's storage requirements for the audit logs will amount to only a few gigabytes per year, so there's no question about efficiency. The ability to play out "what if" scenarios with group permissions is also very useful.

"Being able to identify unused accounts, excessive permissions, unusual or excessive access patterns, and access patterns for individuals that don't match their group patterns are also great features."

—Chuck Klawans, information security officer

I can alter group permissions and instantly see the impact on individual users without actually making the change. The ability to identify unused accounts, excessive permissions, unusual or excessive access patterns, and access patterns for individuals that don't match their group patterns are also great features.

No product is perfect, and I'd like to see Varonis add some new features. It would be great if IP addresses of users accessing resources could be logged. I know Varonis does this for NetApp devices, but the IP address isn't available when other storage devices are used. I asked Varonis about this shortcoming, and it seems to be a technological challenge—the product can report only the information it intercepts from system calls, and this information isn't always available. I'd also like to see information from Active Directory (AD) logs included in reporting, which I think is actually planned for a future release.

What's Hot continues on page 77

Celebrating …

20 YEA

As the world's #1 web host by known servers, we have spent the past 20 years providing cutting edge services and products to millions of users worldwide. We're giving you a chance to start the year successfully by offering discounts on all of our products. Sign up now to take advantage of our special offer and see what a 1&1 website can do for you: www.1and1.com

20 Reasons to use 1&1 …

Top value with market leading prices	Grow your business with free 1&1 Marketing tools	Share photos or create a family page	All-inclusive packages with up to 5 free domains	Enhanced customer communication tools	Showcase your hobbies & interests on a web page	Microsoft® Gold Certified partner	State-of-the-art Data Center	90 day Money Back Guarantee: Details online	Suitable for any level of user


RS
1&1
24/7 Toll-free phone and e-mail support
Powerful, feature-rich servers at attractive prices
Start your own business online
Blog about your interests
Free private domain registration for domains
Use our templates to easily create an appealing website
Seamlessly upgrade your package to fit your growing business
Earn money with 1&1's Affiliate Program
One-Stop-Shop for domains and hosting
NOW 50% off all products for the first 3 months!

Online success starts with a

Using the web is a great way to attract new customers and remind existing customers about your business. Whether you're starting a new business or you've been in business for years, a 1&1 website will help you build a professional image. Find out more about our easy to use 1&1 WebsiteBuilder at www.1and1.com!

50%

website

	1&1 BUSINESS	Yahoo! STANDARD	Go Daddy PREMIUM
Included Domains	3	1	$1.99/year with purchase
Web Space	250 GB	10 GB	200 GB
Monthly Transfer Volume	2,500 GB	400 GB	2,000 GB
E-mail Accounts	2,500 IMAP or POP3	500 POP3	2,000 POP3
Mailbox Size	2 GB	Unlimited	10 MB
Search Engine Submission	✓	✓	Extra charge applies
Website Builder	18 Pages	✓	Freeware
Flash Site Builder	18 Pages	–	–
Photo Gallery	✓	✓	✓
RSS Feed Creator	✓	–	$4.99/month
Ad-free Blog	✓	✓	Freeware
Map & Driving Directions	✓	✓	–
Dynamic Web Content	✓	✓	–
Web Statistics	✓	✓	✓
E-mail Newsletter Tool	✓	$10/month	$3.99/month
In2site Live Dialogue	✓	–	–
Chat Channels	✓	–	✓
Form Builder	✓	✓	–
1&1 Marketing Center	✓	–	–
Premium Software Suite	✓	–	–
90-Day Money Back Guarantee	✓	–	–
Support	24/7 Toll-free Phone, E-mail	24/7 Toll-free Phone, E-mail	24/7 Phone, E-mail
Price Per Month	$5.00 for the first 3 months, after this only $9.99	$19.95	$13.49

*Promotional 50% discount applies to first 3 months of a 12 month contract, after which regular prices will apply. Prices based on comparable Linux web hosting package prices, effective 12/3/2007. Monthly rates shown include discount for annual contract. Product and program specifications, availability, and pricing subject to change without notice. All other trademarks are the property of their respective owners.

Visit our website now to receive 50% off all 1&1 products for the first 3 months!*

1and1.com

or call **1.877.go1and1**

OFF

1&1

50% OFF EVERYTHING!*

20 YEARS 1&1

WEB HOSTING

From $2.00 per month*

DOMAINS

From $6.12 per year**

SERVERS

From $49.50 per month*

MICROSOFT SHAREPOINT(TM)

From $10.00 per month*

1&1 MAIL

From $0.50 per month*

1&1

*Promotional 50% discount applies to first 3 months of a 12 month contract, after which regular prices will apply.
**Price calculated for the full year includes 50% off for the first 3 months.

visit us now **1and1.com** or call **1.877.go1and1**

MEMBER OF united internet

Manage Endpoint Security

Promisec Spectator Professional

I'm the manager of IT security and process at Skadden, Arps, Slate, Meagher and Flom, a large law firm based in New York City. We were in the market for an endpoint security solution, so we reviewed a number of products produced by a variety of vendors. We wanted the ability to monitor the security profiles of all machines on our network from one central location, without affecting users' network performance. After reviewing the available products, we chose **Promisec Spectator Professional**.

Reader:
Nancy M. Lundergan
Manager of IT Security & Process

Product:
Promisec Spectator Professional

Company:
Promisec

Contact:
www.promisec.com

The Spectator console installation is quick and straightforward. Once installed, Promisec supplies you with a unique key for that host and you're ready to scan. Promisec has several helpful features that we use on a regular basis. It's a great benefit that there's nothing to deploy and maintain on local workstations. Another great feature is the ability to run detailed scans during business hours with no impact on local workstations or the network. We've also used Promisec to customize what's allowed on machines from a security perspective; a reporting function breaks down the information we need by host machine and also lists problematic objects. The reporting function gives us the ability to identify problems and deal with them quickly, which is essential to our peace of mind. Promisec updates the definitions for problematic objects monthly, which helps us keep the latest threats off our network.

> "The ability to run detailed scans during business hours with no impact on local workstations or the network is also a great feature."
>
> —Nancy M. Lundergan, manager of IT security & process

The support from Promisec has been great. The company has been quite responsive about incorporating suggestions and requests from users into the product. For example, we needed some sort of indication when a person is in the local admin group on a host, and Promisec added that feature to the next release of the product. Promisec also added the ability to perform enhanced file searches.

InstantDoc ID 97614

DIRECTORY OF SERVICES

Windows IT Pro Network

Search our network of sites dedicated to hands-on technical information for IT professionals.

www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.

www.windowsitpro.com/forums

News

Check out the current news and information about Microsoft Windows technologies.

www.wininformant.com

EMAIL NEWSLETTERS

Get free NT/2000/XP/2003 news, commentary, and tips delivered automatically to your desktop.

- *Windows IT Pro UPDATE*
- *Vista UPDATE*
- *Windows Tips & Tricks UPDATE*
- *WinInfo Daily UPDATE*
- *.NET Briefing*
- *Exchange & Outlook UPDATE*
- *Scripting Central*
- *Security UPDATE*
- *SQL Server 2005 Express UPDATE*
- *SQL Server Magazine UPDATE*
- *Windows IT Library UPDATE*
- *Connected Home EXPRESS*

www.windowsitpro.com/email

PRO VIP ACCESS

Exchange & Outlook Pro VIP

Discover smart solutions for Exchange and Outlook administrators.

www.exchangeprovip.com

Scripting Pro VIP

Learn how to create more powerful scripts and get tips for automating those tedious administrative tasks.

www.scriptingprovip.com

Security Pro VIP

Discover practical, how-to advice for avoiding and solving security problems.

www.securityprovip.com

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Contact Joel Kirk at jkirk@penton.com.

Super CD/VIP

Get exclusive access to all of our print publications, including *Windows IT Pro,* via the new, banner-free VIP Web site.

www.windowsitpro.com/sub/vip

Article Archive CD

Access every article ever printed in *Windows IT Pro* magazine since September 1995 with this portable and speedy tool.

www.windowsitpro.com/sub/cd

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.

www.sqlmag.com

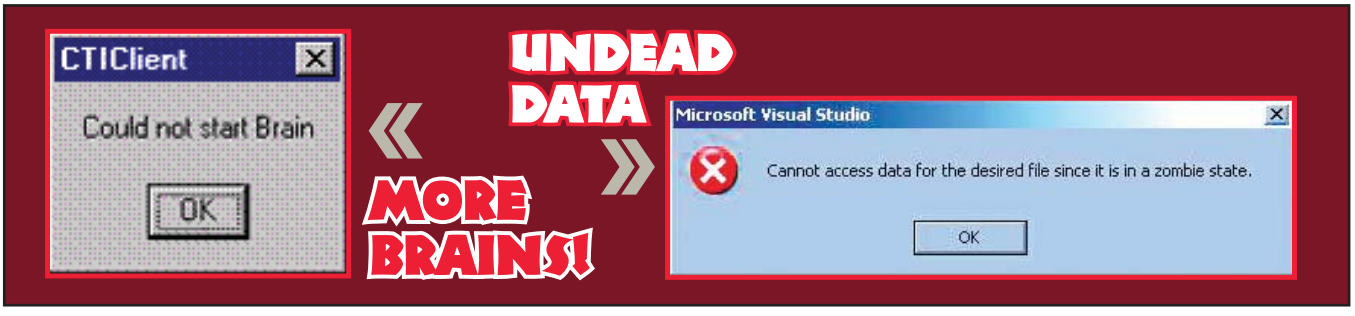
For detailed information about products in this issue of *Windows IT Pro,* visit the Web sites listed below.

VENDOR DIRECTORY

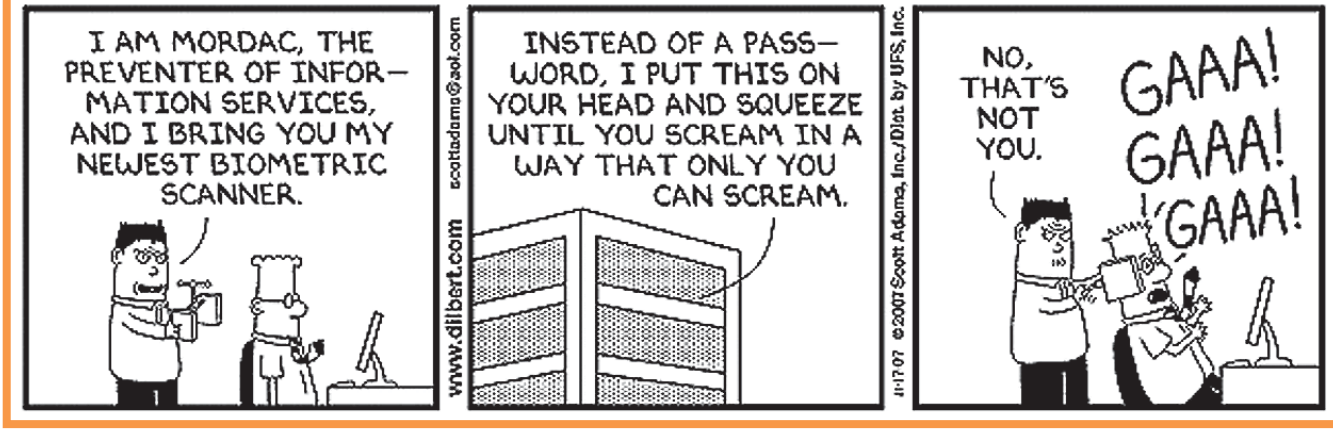
The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

SEND US YOUR INDUSTRY HUMOR! Email your funny screenshots, favorite end-user moments, and humorous IT-related pics to rumors@windowsitpro.com. If we use your submission, you'll receive a Ctrl+Alt+Del coffee mug.

ERRORS OF THE LIVING DEAD



DILBERT® by Scott Adams



January 2008 issue no. 161, *Windows IT Pro* (ISSN 1552-3136) is published monthly. Subscriptions in US, $49.95 for one year; in Canada, $59 US currency, plus 6% for GST for one year; in UK £59; in all other countries, US $99. *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538, (800) 793-5697 or (970) 203-2782. Sales and Marketing Offices: 221 E. 29th St., Loveland, CO 80538. Advertising rates furnished upon request. Periodicals Class postage paid at Loveland, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,* P.O. Box 447, Loveland, CO 80539-0447. SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, P.O. Box 447, Loveland, CO 80539-0447. Printed in the USA. BPA Worldwide Member.

GFI MailSecurity

Complete email security with up to five anti-virus engines for Exchange/SMTP/Lotus

No single anti-virus scanner vendor is the BEST and can stop ALL viruses. To obtain maximum security, you need GFI MailSecurity which uses not one, but up to five virus scanners to check all company email, with limited or no effect on network and server performance.

GFI MailSecurity is better priced than most single anti-virus engine solutions on the market. With multiple anti-virus engines you:

- React fastest to the latest virus threats by receiving the quickest virus signature updates
- Take advantage of all their strengths because no single anti-virus scanner is the BEST
- Virtually eliminate the chances of an infection.

McAfee
NORMAN
bitdefender
AVG Anti-Virus

Download your FREE trial version from www.gfi.com/wmc/

GFI NETWORK SECURITY
CONTENT SECURITY
MESSAGING

tel: +1 (888) 243-4329 | fax: +1 (919) 379-3402 | email: sales@gfiusa.com | url: www.gfi.com/wmc/

ActiveDirectory | Exchange | SharePoint | SQLServer | .NET | SystemCenter | PowerShell

Quest Wins Again!

Microsoft Global ISV Partner of the Year 2004 and 2007

For Windows management, more people think of Quest Software than any other third-party software vendor. And with good reason. Because when it comes to product quality, customer support and a strong partnership with Microsoft, Quest stands alone. That's why Microsoft chose Quest as their Global ISV Partner of the Year for the second time.

Learn why we are the leader in Windows management.
Visit **www.quest.com/ISVaward**

Microsoft GOLD CERTIFIED Partner

2007 GLOBAL ISV PARTNER OF THE YEAR

QUEST SOFTWARE®